

Aberystwyth University

A review of cyber security risk assessment methods for SCADA systems

Cherdantseva, Yulia; Burnap, Pete; Blyth, Andre; Eden, Peter; Jones, Kevin; Soulsby, Hugh; Stoddart, Kris

Published in:
Computers & Security

DOI:
[10.1016/j.cose.2015.09.009](https://doi.org/10.1016/j.cose.2015.09.009)

Publication date:
2016

Citation for published version (APA):

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, 56, 1-27.
<https://doi.org/10.1016/j.cose.2015.09.009>

General rights

Copyright and moral rights for the publications made accessible in the Aberystwyth Research Portal (the Institutional Repository) are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the Aberystwyth Research Portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the Aberystwyth Research Portal

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

tel: +44 1970 62 2400
email: is@aber.ac.uk

Accepted Manuscript

Title: A review of cyber security risk assessment methods for SCADA systems

Author: Yulia Cherdantseva, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, Kristan Stoddart

PII: S0167-4048(15)00138-8

DOI: <http://dx.doi.org/doi: 10.1016/j.cose.2015.09.009>

Reference: COSE 946

To appear in: *Computers & Security*

Received date: 19-5-2015

Revised date: 18-9-2015

Accepted date: 29-9-2015

Please cite this article as: Yulia Cherdantseva, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, Kristan Stoddart, A review of cyber security risk assessment methods for SCADA systems, *Computers & Security* (2015), <http://dx.doi.org/doi:10.1016/j.cose.2015.09.009>.

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.



A Review of Cyber Security Risk Assessment Methods for SCADA Systems

Yulia Cherdantseva¹, Pete Burnap

School of Computer Science and Informatics, Cardiff University, UK; email:

y.v.cherdantseva, burnapp@cs.cardiff.ac.uk

Andrew Blyth, Peter Eden

Faculty of Computing, Engineering and Science, University of South Wales, UK; email:

andrew.blyth, peter.eden@southwales.ac.uk

Kevin Jones, Hugh Soulsby

Cyber Operations, Airbus Group Innovations, UK; email: kevin.jones,

hugh.soulsby@eads.com

Kristan Stoddart

Department of International Politics, Aberystwyth University, UK; email:

kds@aber.ac.uk

Abstract

This paper reviews the state of the art in cyber security risk assessment of Supervisory Control and Data Acquisition (SCADA) systems. We select and in-detail examine twenty-four risk assessment methods developed for or applied in the context of a SCADA system. We describe the essence of the methods and then analyse them in terms of aim; application domain; the stages of risk management addressed; key risk management concepts covered; impact measurement; sources of probabilistic data; evaluation and tool support. Based on the analysis, we suggest an intuitive scheme for the categorisation of cyber security risk assessment methods for SCADA systems. We also outline five research challenges facing the domain and point out the approaches that might be taken.

Keywords: SCADA, cyber security, risk assessment, risk analysis

1. Introduction

A Supervisory Control and Data Acquisition (SCADA) system is a type of Industrial Control System (ICS). An ICS controls processes in the industrial sector and in the sectors which form a Critical National Infrastructure (CNI) **Error! Reference source not found..** The list of sectors forming CNI varies from country to country. In the UK, CNI is defined as “*Those infrastructure assets (physical or electronic) that are vital to the continued delivery and integrity of the essential services upon which the UK relies, the loss or compromise of which would lead to severe economic or social consequences or to loss of life*” and is formed by nine sectors: energy, food, water, transportation, communications, emergency services, health care, financial services and government **Error! Reference source not found..**

SCADA systems stand out among other ICSs as systems that (1) monitor and control assets distributed over large geographical areas, and (2) use specific control equipment such as a Master Terminal Unit (MTU) and Remote Terminal Unit (RTU), which we further discuss in Section 2. Initially, SCADA systems were used in power transmission, gas pipeline and water distribution control systems. Nowadays, SCADA systems are widely used in steel making, chemistry, telecommunications, experimental and manufacturing facilities [2, 4, 6].

The smooth and reliable operation of SCADA systems is vital for such sectors of

¹Corresponding author

CNI as energy, water and transportation where both data acquisition and control are critically important. A widespread, long-lasting outage of SCADA and, consequently, CNI may cause serious disturbance to a state and society [6, 11]. The consequences of a malfunction of a SCADA system may be detrimental and may range from financial loss due to an equipment and environmental damage to the loss of human life **Error! Reference source not found..**

Security in general and cyber security specifically were not the major concerns of early standalone SCADA systems **Error! Reference source not found..** Security was primarily achieved by controlling physical access to system components which were unique and used proprietary communication protocols. For years, security in SCADA systems was present only as an implication of safety. Over the last decade, however, the situation has changed, and a number of standards and directives dealing with the cyber security of SCADA systems have emerged.

In 2004, the National Institute of Standards and Technology (NIST) published the document titled *System Protection Profile - Industrial Control Systems* which covers the risks and objective of SCADA systems **Error! Reference source not found..** In 2005, the National Infrastructure Security Coordination Center (NISCC), a predecessor of the Centre for the Protection of National Infrastructure (CPNI) in the UK, published a good practice guide for firewall deployment in SCADA networks **Error! Reference source not found..** In 2007, the US President's Critical Infrastructure Protection Board and the Department of Energy outlined the steps an organisation must undertake to improve the security of its SCADA networks in the booklet *21 Steps to Improve Cyber Security of SCADA Networks* **Error! Reference source not found..** In 2008, the Centre for Protection of National Infrastructure (CPNI) produced a *Good Practice Guide for Process Control and SCADA Security* **Error! Reference source not found.** encapsulating best security practices. In 2008, NIST released a comprehensive guidance on a wide range of security issues, and technical, operational and management security controls. The guide was updated in 2011 **Error! Reference source not found..** In 2013, the European Union Agency for Network and Information Security (ENISA) released the recommendations for Europe on SCADA patching **Error! Reference source not found..** Currently, the North American Electric Reliability Corporation (NERC) actively works on the development of a wide range of standards covering many aspects of CNI cyber security **Error! Reference source not found..** More extensive overviews of SCADA-related security standards and initiatives are provided in [2, 12].

Modern day SCADA systems are highly sophisticated, complex and based on advanced technology systems. The escalating sophistication and modernisation as well as real-time continuous operation and distributed, multi-component architecture underpin the growth of cyber threats to SCADA systems. SCADA systems are exposed to a wide range of cyber threats also because of the standardisation of communication protocols and hardware components, growing interconnectivity and legacy. (All these aspects we discuss in greater detail in Section 2.)

Over the last several decades we already saw a range of cyber attacks on CNI and SCADA. In 1982, the first recorded cyber attack on CNI took place at the Trans-Siberian pipeline and resulted in an explosion visible from space **Error! Reference source not found..** Over the last decade there was a number of

cyber attacks on SCADA systems and ICS. In 2003, a slammer worm penetrated a network at the Davies-Besse nuclear plant in Ohio [8, 11] and a computer virus named Sobig shut down train signalling systems in Florida **Error! Reference source not found..** In 2006, a hacker penetrated the operation system of a water treatment facility in Harrisburg, USA [8, 11] and the Browns Ferry nuclear plant in Alabama was manually shut due to the overload of network traffic **Error! Reference source not found..** In 2007, a dismissed employee installed unauthorised software on the SCADA system of the Tehama Colusa Canal Authority **Error! Reference source not found..** In 2010, the Stuxnet computer worm struck the Iranian nuclear facility causing the failure of almost one-fifth of all centrifuges **Error! Reference source not found..** Stuxnet was a game-changer, it attracted the world's attention to cyber threats to CNI by drawing a vivid and horrifying picture of the consequences of a cyber attack on CNI. In 2011, five global energy and oil firms were targeted by a combination of attacks including social engineering, trojans and Windows-based exploits **Error! Reference source not found..** In 2012, a malware named Flame was discovered to have been operating in many sites in the Middle East and North Africa for at least two years **Error! Reference source not found..** A larger number of cyber attacks on CNI is listed and analysed in [10, 12].

The analysis in **Error! Reference source not found.** indicates that the number of cyber attacks on CNI increases over time. The number of SCADA-related incidents also steadily grows. In 2010, the Repository of Industrial Security Incidents (RISI) had 161 incidents listed with about 10 new incidents being added each quarter **Error! Reference source not found..** In 2013, the RISI database contained already 240 incidents recorded between 2001 and the end of 2012 **Error! Reference source not found..** Additionally, an extensive study of the current cyber security state of SCADA systems based on a set of interviews with a large number of experts confirmed that cyber threats in SCADA systems are escalating, they are “*real and expanding*” **Error! Reference source not found..**

All the above stipulates the strong need for the effective management of cyber security risks in SCADA systems. Risk assessment is an important part of the best practice risk management in ICS and SCADA systems [13, 15]. Risk assessment answers the following three questions **Error! Reference source not found.:**

- What can go wrong?
- What is the likelihood that it would go wrong?
- What are the consequences?

Risk management builds upon the risk assessment in order to answer the other three questions **Error! Reference source not found.:**

- What can be done and what options are available?
- What are the associated trade-offs in terms of all costs, benefits, and risks?
- What are the impacts of current management decisions on future options?

A range of standards and normative documents attending to risk management and risk assessment has been devised over the years for IT systems. ISO 31000:2009 **Error! Reference source not found.** outlines generic, non-industry-specific guidelines on risk management. NIST SP 800-30 contains a guide on risk management for IT systems **Error! Reference source not found..** NIST 800-37 **Error! Reference source not found.** provides a risk management framework for

federal information systems. ISO/IEC 27005:2011 **Error! Reference source not found.** is a standard for information security risk management.

A range of general IT risk assessment methodologies is used in industry: Operationally Critical Threat and Vulnerability Evaluation (OCTAVE) **Error! Reference source not found.**, Central Computer and Telecommunications Agency Risk Analysis and Management Method (CRAMM) **Error! Reference source not found.**, Consultative, Objective and Bi-functional Risk Analysis (COBRA) **Error! Reference source not found.** and CORAS [49, 50], a model-based risk assessment methodology for security-critical systems. Also there is a broad range of academic proposals such as for example Information Security Risk Analysis Method (ISRAM) **Error! Reference source not found.**, COst estimation, Benchmarking, and Risk Assessment (COBRA) **Error! Reference source not found.**, SPRINT, a simplified practical risk analysis methodology **Error! Reference source not found.**, and the Business Process: Information Risk Management (BPIRM) methodology **Error! Reference source not found.** to name just a few.

While a large number of IT risk assessment methodologies exists, the specifics of SCADA systems as opposed to IT systems, which are discussed in Section 2, often prevent the straight forward application of risk assessment methods designed for corporate IT systems to SCADA systems. An IT risk assessment method must be adjusted to fit the context of SCADA systems.

In the general context, risk is described as follows **Error! Reference source not found.**:

$$R = \{s_i, p_i, x_i\}, i = 1, 2, \dots, N \quad (1)$$

where

- R - risk;
- $\{\}$ - must be interpreted as a “set of”;
- s - a scenario (undesirable event) description;
- p - the probability of a scenario;
- x - the measure of consequences or damage caused by a scenario; and
- N - the number of possible scenarios that may cause damage to a system.

In the context of a SCADA system, risk “*is a function of the likelihood of a given threat source exploiting a potential vulnerability and the resulting impact of a successful exploitation of the vulnerability*” [1, Sec. 6.1.3]. When applied to quantifying cyber security risks in SCADA systems the formula for calculating risk is accepted as follows **Error! Reference source not found.**:

$$R = t \vee x_{tv}, \quad (2)$$

where

- t - threat;
- v - vulnerability; and
- x_{tv} - the consequences of the threat successfully exploiting the vulnerability.

Risk assessment in SCADA systems shall help to prioritise (1) the components of a system in terms of their importance to the successful operation of the system or in terms of their level of vulnerability to an attack, and (2) threats in terms of the danger they pose and their likelihood. Risk assessment shall assist the managers and engineers of SCADA

systems with the development of adequate security policies, with the design of secure system and with the rational allocation of often scarce resources **Error! Reference source not found.** It shall also facilitate the communication between security, business and SCADA experts.

In 2004, it was stated that “[t]here is an urgent need for a systemic risk-based methodology that would add protection to SCADA systems, given their central role in controlling and operating critical interdependent infrastructure systems” [23, p.18]. During the past ten years a number of risk assessment methodologies for SCADA systems were proposed. Driven by the importance of managing and assessing cyber security risks in SCADA systems, *the ultimate aim of the paper at hand is a comprehensive, structured and detailed review of existing cyber security risk assessment methods specifically tailored for SCADA systems.*

Several relevant literature reviews exist. Reviews covering SCADA security and cyber security issues are presented in [2, 6, 12, 13], but these reviews do not concentrate on risk assessment methods. In **Error! Reference source not found.**, twenty-one risk assessment methodologies for CNI proposed by various commercial and organisations are surveyed; however, **Error! Reference source not found.** does not concentrate on SCADA systems. In **Error! Reference source not found.**, only a brief description of several risk assessment methodologies for the oil and gas sector is outlined. An extensive overview of risk assessment methodologies is contained in **Error! Reference source not found.**, but only two methods are examined in detail. This review paper updates and significantly extends the overview of risk assessment methods in **Error! Reference source not found.**, which was published in 2007. Our review devotes equal attention to every method examined. To the best of our knowledge, this paper provides the most comprehensive and detailed overview of cyber security risk assessment methods applied in the context of SCADA systems.

Another aim of the paper is to examine the advantages and drawbacks of the existing cyber security risk assessment methods for SCADA systems. This analysis forms a solid foundation upon which new risk assessment methods for SCADA systems might draw and the existing ones might be improved.

Risk assessment methods in general and in the context of SCADA systems specifically are hard to categorise as we conclude based on our analysis and in agreement with [6, 7]. A categorisation scheme must be multilateral and must focus attention on the different aspects of methods. The development of a comprehensive, yet intuitive categorisation scheme remains an open research question. A categorisation scheme may assist with (1) the search and review of relevant methods, (2) the identification of similar or duplicating methods, and (3) the elaboration of the common characteristics of the methods of the same category. The latter might enable a sound analysis of methods within a category.

Based on the comprehensive review, in this paper we propose an intuitive categorisation of cyber security risk assessment methods for SCADA systems. On one lateral, we split the methods examined into guidelines, activity-specific methods and elaborated guidelines. On another lateral, we categorise methods into model-based and formula based.

The detailed description of examined methods, their thorough analysis and intuitive classification scheme presented in this paper aim to provide guidance for and

assist practitioners with the choice of an appropriate risk assessment method. The review examines the application domain of the methods, their aims, key concepts and stages of risk management addressed. We also discuss the sources of probabilistic data used by the methods, how the impact is measured, how the methods are evaluated and whether tool support is provided. The drawbacks of widely-used probabilistic risk assessment methods are also revealed to the reader.

As the outcome of our review, we describe current research challenges in cyber security risk assessment in SCADA systems and point out to possible approaches that can help future work in this area. Research communities and practitioners dealing with risk management in SCADA systems may benefit from this discussion.

The remainder of the paper is organised as follows. In Sections 2, in order to arm the reader before exposing him/her to the review we provide some background discussion on what SCADA systems are and on security challenges facing them. Then, in Sections 3 we describe the review methodology. Section 4 provides the reader with the brief descriptions of all methods examined. We found it necessary to present these descriptions prior to the analysis as the knowledge of separate methods leads to the better appreciation of the review results. Section 5, contains the summary analysis of the methods examined and key findings that stem from it. Finally, Section 6 outlines research challenges facing the domain of cyber security risk assessment in SCADA systems in future. We draw some concluding remarks in Section 7.

2. SCADA Systems and Cyber Security Challenges

A SCADA system consists of hardware and software components, and of a connecting network(s). Figure 1 shows a generic hardware architecture of a SCADA system. An architecture is formed by one or more control centres and a number of field devices such as an RTU, Intelligent Electronic Device (IED) and Programmable Logic Controller (PLC) connected by a communication infrastructure. An RTU receives data from field devices, converts it to digital data and sends it to the control centre as well as receives digital commands from the centre and handles alarms. A PLC is a digital computer that monitors sensors and takes decisions based upon a user created program to control valves, solenoids and other actuators. A control centre includes an MTU, which issues commands to and gathers data from RTUs, it also stores and processes data in order to display information to human operators to support decision making. Human operators monitor and control the system from a control center via Human-Machine Interface (HMI) displays.

Communication on a SCADA network is paramount. Messages are exchanged (1) between master devices, which control operation of other devices (e.g. PLCs) and slave devices (e.g. sensors, actuators, relays), which send messages to master devices and perform actions at their command, and (2) between field devices using a peer-to-peer communication model **Error! Reference source not found..** The following communication protocols are used in SCADA systems: Ethernet/IP, DeviceNet, ControlNet, PROFIBUS, MODBUS TCP/IP, DNP3 and Foundation Fieldbus [2, 5]. As they cover large geographical areas, SCADA systems typically use Wide Area Networks (WAN). The communication infrastructure may be satellite, radio, power line based and any combination of the above.

The software in SCADA systems is multi-tasking, uses real-time database(s) and typically provides the following functionality: the display of synoptic diagrams and text

as well as a possibility to view them on multiple screens, general editing (e.g. re-sizing and scrolling), trend analysis, alarm handling, logging, archiving, report generation and the automatic triggering of control actions **Error! Reference source not found.**

Following advances in Information and Communication Technology (ICT), over the last two decades the architecture of a SCADA system has become more open with a large number of commercial off-the-shelf hardware and software relying upon standardised communication protocols being used. The reasons for these changes in a SCADA architecture are, among others, financial. The use of off-the-shelf components and open communication protocols leads to a significant cost reduction. The number of proprietary design and implementation activities to be carried out by an end-user decreases. Technical support and maintenance are provided by a vendor eliminating the need for an in-house support team.

The use of standardised communication protocols enables the integration of a SCADA system with a corporate IT system and its connection to the Internet. The increased interconnectivity of SCADA systems simplifies their maintenance and control: *“You are a manager at a municipal utility. A few years ago, when the beeper signaled an alarm well past midnight, you had to drape a raincoat over your pajamas, jump into your car and race to the plant. Once there, you ran down to the basement and flipped some switches. Nowadays, you reach for your tablet or smart phone and tap some icons without leaving your warm and cozy bed”* **Error! Reference source not found.**

SCADA systems must adjust to interconnectivity as did corporate IT systems at the early days of the Internet. However, SCADA are different from business information systems in many ways. SCADA systems are time critical and geographically distributed, they support complex interactions between physical and logical infrastructures while operating continuously, the effect of malfunction is more tangible while access to the various components of a system is more complicated, and the life time of system components is usually 3 to 4 times longer. NIST SP 800-82 [1, Sec.

3.1], **Error! Reference source not found.**, **Error! Reference source not found.**

and **Error! Reference source not found.** discuss the differences between IT systems and ICS in greater detail.

The specifics of SCADA systems lead to the fact that not all security countermeasures exploited in IT systems are applicable to SCADA systems. In fact, some countermeasures may damage a SCADA system more than secure it. On the one hand, security countermeasures such as access control, VPN and firewall, which have already demonstrated their efficiency in the IT security domain, are also successfully adopted by SCADA systems **Error! Reference source not found.** On the other hand, countermeasures such as authentication and cryptography must be used with an extreme caution because they may have a disruptive effect on the operation of a SCADA system where every action is time critical. In **Error! Reference source not found.**, it is discussed how traditional IT security countermeasures may be exploited in SCADA systems avoiding negative impact on system safety and efficiency.

For over forty years confidentiality, integrity and availability - also referred to as the CIA-triad - have been defining the set and priorities of security goals for corporate information systems. In ICS and SCADA systems, the priorities among the goals are different. Among the triad, integrity and availability are highly paramount, while confidentiality is secondary for SCADA systems [13, 18]. In reality, security goals, in

what ever order they appear, are often preceded in SCADA systems by safety, reliability, robustness and maintainability (which are the supreme goal of critical systems) leaving little or no resources for security goals. In **Error! Reference source not found.**, the authors discuss a need for an update of such well established international security standards as NIST SP 800-53 and ISO 27001 in order to address the specifics of ISC is stated. A new standards, according to **Error! Reference source not found.** shall be bring together the CIA-traid and safety requirement critical in the context of an ICS.

Cyber security issues in SCADA systems are further exacerbated by the legacy problem. Existing SCADA systems, due to their continuous operation, are not updated or re-designed in some cases for decades. The nature of SCADA systems requires them to be operational 24 hours 7 days a week. This makes the regular patching and upgrading of both a SCADA software and a hosting operating system difficult, if not impossible [12, 13]. The patching of a SCADA system is complicated by the facts that the system is time-critical, there is no test environment and patching may introduce new unknown vulnerabilities or ultimately break the system. Legacy SCADA system may end up relying on operating systems and software that are no longer supported by vendors **Error! Reference source not found.**

The human factor plays a momentous role in cyber security of SCADA systems. Human supervision, and complicated software architecture and development process are the characteristics of SCADA systems which exacerbate the role of the human factor **Error! Reference source not found.** An eternal vigilance regarding human factor helps with the prevention of human errors which may result in unintended attacks, and with the prevention of intended internal and external social engineering attacks. Attacks by internal agents, i.e. employees of an organisation, are more often than attacks by external ones **Error! Reference source not found.** The increased sophistication of SCADA systems calls for highly knowledgeable and well-trained personnel. Despite the need, proper training for people working with SCADA systems often comes short in practice **Error! Reference source not found.** The study of the role of the human factor in cyber security of SCADA systems started to gain momentum over the last decade [23, 6].

3. Review Methodology

The scope of the literature review conducted was as follows. The original set of papers was formed from the searchers run on IEEE Xplore, ACM, SCOPUS and Web of Science as recommended in **Error! Reference source not found.** IEEE Xplore and ACM provide a good coverage of relevant journals and conferences. SCOPUS and Web of Science are two general indexing systems. The search string was constructed from the keywords “SCADA” and “risk assessment”. The search covered the period of ten years between 2004 and 2014. The search was performed in November 2014 and returned for ACM Digital Library, IEEE Xplore, SCOPUS and Web of Science (Core Collection) 36, 14, 105 and 14 papers respectively. The resulting set of papers undergone manual reduplication. Next, papers were selected for review manually based on the examination of the title, abstract and full text where it was readily available or where the information provided in the abstract was not sufficient. We also ensured that all papers relevant to the subject of this review mentioned in the review papers covering security and risk in SCADA, namely [2, 6, 12, 13], are included in our analysis.

As a general rule, we included in the review the papers which suggested a new method covering at least one of the stages of a risk assessment process and where a

method was specifically developed for or applied to a SCADA system. The papers which are dedicated to security requirements derivation, but are not written in the context of risk assessment (e.g. **Error! Reference source not found.**) as well as the papers addressing vulnerability analysis from the technical rather than the risk management perspective (e.g. [41, 42]) were not included in our review. We focused only on research publications dealing primarily with cyber security or information security, while the papers covering risk assessment from the safety or reliability perspectives only (e.g. **Error! Reference source not found.**) were excluded out of the review. This was done in order to keep the scope of our analysis in such a breadth where it is possible to examine each method in detail rather than superficially. Furthermore, such topics as safety and reliability in the context of SCADA are very broad and complex, and are typically studied by different research communities.

Arguably, many IT risk assessment methodologies with some adjustments may be applied to SCADA systems with various degree of success. However, to what degree IT methods are fit for SCADA systems and what adjustments they need remain open research questions. Therefore, in this paper, we examined only those risk assessment methods which were developed for or already applied to SCADA systems. We avoided conjecturing about the applicability of corporate IT risk assessment methods to SCADA systems.

Finally, 24 papers, each presenting a risk assessment method for a SCADA system, were selected for the analysis in this review paper. The methods were examined according to the following criteria:

1. Aim;
2. Application domain;
3. Stages of risk management addressed;
4. Key concepts of risk management covered;
5. Impact measurement;
6. Sources of data for deriving probabilities;
7. Evaluation method; and
8. Tool Support.

In the following section, the essence of each risk assessment method selected for analysis is epitomised. We describe the methods in a chronological order. This is followed by the discussion and summary analysis of the methods in Section 5.

Before we proceed with the description and analysis of the methods, the limitations of the review process must be noted. First, the analysis was done based only on our interpretation of the papers. We did not contact the authors of the methods to verify the correctness of our understanding. Second, as with any literature review, it was not possible to exclude the factor of subjectivity while selecting and analysing methods. Facing up this issue, we made the selection and analysis process transparent by thoroughly documenting it. Third, we did not specifically trace for each method analysed whether there is a follow up on the method from one of the authors unless a follow up paper appeared among the papers selected for analysis or the existence of a follow up paper was mentioned in the paper examined. Finally, we cannot completely rule out the existence of other relevant unobserved risk assessment methods for SCADA systems. Some proposals may have not found their place in the review due to various reasons: a terminology used by authors which did not bring a paper in to the radar of our analysis, a

paper not being listed on the databases examined, the subjectivity factor, and time and resource restrictions on the report production. Nevertheless, the literature search method adopted helped to ensure an acceptable level of the completeness of our literature review. Hence, we believe that the set of papers analysed is representative and the results of the analysis may be generalised for the domain.

4. Description of Risk Assessment Methods for SCADA

4.1. Risk Assessment in SCADA for Railways,

2004 **Error! Reference source not found.**

A risk assessment framework which utilises the Hierarchical Holographic Modelling (HHM) and is designed for GPS-based railway SCADA systems is described in **Error! Reference source not found.**

HHM is the methodology for “capturing and representing the essence of the inherent diverse characteristics and attributes of a

system” **Error! Reference source not found.** HHM was used for modelling complex defence and civilian systems. It aids in assessing risks in sub-systems and their effect on the system as a whole, which makes HHM useful in the context of

SCADA **Error! Reference source not found.**

Three sub-models are distinguished in the hierarchical holographic model of a SCADA system **Error! Reference source not found.**: (1) hardware and software, (2) human supervisory and (3) environment. Each of these sub-models is decomposed into elements and each element is decomposed into subtopics.

The framework suggests to map the Control Objectives for Information and Related Technology (CobiT) onto the holographic model in order to facilitate risk identification.

4.2. Attack Trees for Assessing Vulnerabilities in SCADA,

2004 **Error! Reference source not found.**

In **Error! Reference source not found.**, attack trees are used to assess vulnerabilities in SCADA systems based on MODBUS and MODBUS/TCP communication protocols. An attack tree provides a structured view of events leading to an attack and, ultimately, helps with the identification of appropriate security countermeasures.

Risk, according to **Error! Reference source not found.**, depends on: (1) system architecture and conditions; (2) countermeasures in place; (3) attack difficulty; (4) detection probability; and (5) attack cost. The purpose of the assessment

in **Error! Reference source not found.** is to calculate the characteristics of the topmost attack event and to identify possible ways to achieve the final goal of the attack. In order to achieve this, first, a team of industry experts identifies possible goals of an attacker and designs an attack tree with goals depicted as the nodes of the tree. Then, each leave of an attack tree is assigned a level of technical difficulty on the scale

“Trivial-Moderate-Difficult-Unlikely”. Based on two functions - AND as the maximum of the children nodes values and OR as the minimum of the children nodes values - the difficulty of each node that has children nodes is calculated. The difficulty rating may vary over time.

Each goal is also characterised by the severity of impact it may cause and by the

probability of detecting malicious activity associated with this goal. Both indicators are also defined on relative scales.

The paper presents a sample attack tree for a MODBUS-based SCADA system (Figure 2). The trees in **Error! Reference source not found.** were designed by the team of industry experts and the feasibility of the attacks was tested in a laboratory settings.

4.3. *Vulnerability Assessment Methodology for SCADA Security, 2005* **Error! Reference source not found.**

A cyber vulnerability assessment methodology for SCADA systems in **Error! Reference source not found.** is based upon the experience of assessing the security of multiple SCADA systems conducted as a part of the national SCADA Test Bed program sponsored by the Department of Energy - Office of Electricity and Energy Assurance, US and the Idaho National Laboratory SCADA Test Bed program.

The methodology described in **Error! Reference source not found.** consists of five steps:

1. Assessment plan development: a plan outlines budget, schedule, goals, resources and the engagement of experts required, and deliverables expected from an assessment.
2. Testing environment configuration: the testing environment must be safe and non-production configuration.
3. Vulnerability assessment: the vulnerability assessment is performed via a penetration test conducted from an external to the tested system machine. A range of open source and commercial tools for assessing system vulnerability is listed.
4. Reporting: the methodology of assessment and testing along with the results must be thoroughly documented.
5. Metrics and scoring: the security of SCADA system must be measured quantitatively so that it may be benchmarked against other systems.

4.4. *Quantitative Cyber Risk Reduction Estimation Methodology, 2006* **Error! Reference source not found.**

McQueen et al. **Error! Reference source not found.** suggest a methodology for the quantitative estimation of cyber risk reduction for a SCADA system in which an enhancement of cyber security has been performed. For risk reduction estimation a directed graph of a cyber attack is developed for both a baseline and improved systems, and the difference in time-to-compromise each system is measured and analysed.

The methodology consists of ten steps:

1. Establish system configuration;
2. Identify the applicable portions of the quantitative risk model;
3. Identify and prioritise the security requirements of the primary target(s);
4. Identify system vulnerabilities;
5. Categorise vulnerabilities on each device by the type of compromise;
6. Estimate time-to-compromise for each device;
7. Generate compromise graph(s) and attack paths;
8. Estimate dominant attack path(s);
9. Perform steps 3-8 for both baseline and enhanced system; and
10. Compare results of both version of the system and estimate risk reduction.

McQueen et al. **Error! Reference source not found.** introduce a formula for

calculating the probability of an occurrence of an undesired event. This probability is the product of the following conditional probabilities: the probability of the system being on an attacker's target list, the probability of being attacked given that the system is targeted, the probability of a perimeter breach given that the system is attacked, the probability of a successful attack given that there is a perimeter breach and the probability of damage given the system is successfully attacked. Since the estimation of all probabilities involved is not feasible, risk reduction is measured as the change of the probabilities of perimeter breach and successful attack rather than an absolute value of risk.

Security requirements for SCADA are identified so that integrity and availability have the highest priority, while confidentiality is secondary. The vulnerabilities of a system are identified using existing vulnerability identification libraries. Each vulnerability is classified as reconnaissance, breach, penetrate, escalation or damage. Time-to-compromise a device is calculated. It depends on the known vulnerabilities of the target system and the skills of an attacker. A circumstantial discussion of the methods for estimating time-to-compromise could be found

in **Error! Reference source not found..**

A compromise graph, where each node indicates a potential attack state, is developed for the baseline and enhanced SCADA systems, and the dominant paths of attack are chosen as the paths which require minimum time-to-compromise the target system. Finally, time required to compromise the baseline and enhanced system is compared. Time-to-compromise here is used as the main indicator of system security and risk.

For the evaluation purposes, the proposed methodology is applied to a small-size SCADA system for measuring the effectiveness of security countermeasures.

4.5. *Vulnerability Assessment of Cyber Security in Power Industry, 2006* **Error! Reference source not found.**

Two formulas for the probabilistic assessment and integrated risk assessment of cyber security vulnerability in SCADA systems, Energy Management Systems and Management Information Systems are proposed in **Error! Reference source not found..**

The vulnerability index of the cyber security of a system is calculated as follows:

$$I_e = \sum_{j \in N} P(E_j) \times P(EL_j / E_j) \times L_j(EL_j) \quad (3)$$

where

$P(E_j)$ is the probability of the occurrence of event E_j ;

$P(EL_j / E_j)$ is the probability of power system accident EL_j resulting from cyber security event E_j ; and

L_j - the loss caused by accident EL_j .

It is not clear from the paper, how the probability of a security event is estimated, it is only mentioned that the probability is Poisson distributed.

4.6. *Scenario-based Approach to Risk Analysis in Support of Cyber Security, 2006* **Error! Reference source not found.**

A scenario-based approach to cyber risk assessment used by the Control Systems Security Center (CSSC) for the National Cyber Security Division of the Department of Homeland Security is described in **Error! Reference source not found..**

The scenario and risk assessment process consists of ten activities: 1) identify key

infrastructure; 2) identify representative mid-level processes; 3) determine consequences levels; 4) develop process flow diagrams with key components, structures and systems; 5) review underlying safety analysis and operating history; 6) review threat and vulnerability data; 7) develop likely attack pathways and key human-system responses; 8) compute probabilities and assess quantifiable resultant damage state; and 10) document findings, assess limitations and produce uncertainty characterisation.

The system under examination was modelled by experts familiar with industrial process and security requirements. Vulnerabilities and threats as well as expected human-system response were reviewed by operation experts, while probabilities and possible ways of attacks were defined by cyber experts. The opinion of experts were captured using the Delphi technique. As a part of the scenario-based method attack variations, skills required by an attacker and potential system effects were elaborated for a particular cyber attack scenario on a nuclear plant.

4.7. *Two Indices Method for Quantitative Assessment of the Vulnerability of Critical Information Systems, 2008* **Error! Reference source not found.**

Another method for the qualitative assessment of the vulnerability (security level) of a SCADA system is suggested in **Error! Reference source not found.**. The method helps system managers to make more informed decisions about security countermeasures to be implemented.

The method is based on a vulnerability tree augmented with two indices, namely threat-impact index and cyber-vulnerability index. The threat-impact index reflects a financial effect of a cyber threat: a higher index indicates a higher impact. The cyber-vulnerability index reflects the vulnerability of a system with regard to cyber attacks. A more vulnerable system has a higher index. Both indices are measured on the scale from 0 to 100.

The method requires five steps to be undertaken:

1. Development of the base-level and expanded vulnerability trees for an original system;
2. Population of an effect analysis table and calculation of threat-impact index values;
3. Augmentation of the tree with threat-impact index values;
4. Calculation of cyber-vulnerability index values;
5. Augmentation of the tree with cyber-vulnerability index values; and
6. Reproduction of steps 2 to 5 for a security-enhanced system and the comparison of results.

The vulnerability tree presented in **Error! Reference source not found.** was developed based on the analysis of attacks launched in the past. Financial losses caused by attacks were estimated by interviewing engineers, managers, operator and accountants. The probabilities of attacks were identified based on historical data. The method was applied to a test SCADA system at the University of Louisville.

4.8. *Cyber-Terrorism SCADA Risk Framework, 2009* **Error! Reference source not found.**

In **Error! Reference source not found.**, a cyber-terrorism SCADA risk framework which is validated by a focus group of five SCADA industry experts is presented. The framework consists of three stages: (1) risk assessment, (2) capability assessment model,

and (3) controls.

The recommendation for the risk assessment stage is to adjust the AS/NZS 4360:2004, an Australian risk management standard, for the specifics of SCADA systems. For the development of the cyber-terrorism capability assessment model, the level of cyber-terrorist group capability is characterised using eight indicators: (1) advanced ICT skills, (2) advanced hacking tools and techniques, (3) access to new advanced ICTs, (4) advanced knowledge of SCADA systems, (5) insiders within the organisation of a selected target, (6) reconnaissance, (7) funding, and (8) motivation.

The controls stage adopts another Australian standard AS/NZS 27002:2006 for information security management and adjusts it to the SCADA context listing eleven security control clauses:

1. SCADA Security Policy,
2. SCADA Physical and Environmental Security,
3. SCADA Organisation Information Security,
4. SCADA Asset Management,
5. SCADA Human Resources Security,
6. SCADA Communications and Operations Management,
7. SCADA Access Control,
8. SCADA Information Systems Acquisition, Development and Maintenance,
9. SCADA Information Security Incident Management,
10. SCADA Business Continuity Management, and
11. SCADA Compliance.

4.9. *Evaluating the Risk of Cyber Attacks on SCADA Systems via Petri Net Analysis, 2011* **Error! Reference source not found.**

A methodology for quantifying the risk of cyber attacks on computer network operations on SCADA systems is introduced in **Error! Reference source not found.** The method is based on the Petri Net state coverability analysis and process simulation. The purpose of the method is to identify all high-consequence attack states. The method avoids the use of such measure as likelihood since it is “*difficult to credibly evaluate in many practical applications*”, but rather represents risk as “*a function of the resources to which an attacker can gain access during an attack*” **Error! Reference source not found.** The method is demonstrated on a non-automated hazardous liquid loading process which is described in **Error! Reference source not found.**

For the purpose of analysis, first, potential process failure modes with corresponding consequences are identified and from them those failure modes are separated which may lead to a process failure. Then, the resources needed by an attacker to commit an attack are identified. As a result, three Petri net models are designed: industrial process model, SCADA operation model and resource-vulnerability topology. The resources available to an attacker form prerequisites for a SCADA failure, which in its turn may result in one or more process failures. Consequences may be measured in a metric meaningful to process owners. As examples such possible metrics as lost production throughput and environmental pollution are mentioned. In the example provided in the paper, the severity of impact is measured in terms of the number of injures to the personnel serving the process.

Two risk metrics are proposed in **Error! Reference source not found.**: (1) center of mass risk measure, which is the median of the set of the consequence of all inducible SCADA and process failure modes; and (2) worst-case risk measure, which is a maximum value of the set. Six types of failure modes are adopted from **Error! Reference source not found.**

4.10. *Hierarchical, Model-Based Risk Management of Critical Infrastructures*, 2009 **Error! Reference source not found.**

In **Error! Reference source not found.**, an approach to risk management based on a set of the hierarchical labelled hypergraphs of the security dependencies between the components of an infrastructure is elaborated.

In this approach an infrastructure hypergraph and an evolution graph, which may be regarded as a more detailed variation of an attack graph, are developed. An infrastructure hypergraph is a model of the interdependent components of a system depicting the internal states of components and operations on them. An evolution graph is a directed acyclic graph which consists of the states of an elementary attack committed to achieve a final goal. Each evolution describes an attack strategy. For analysis, an evolution graph is pruned to remove all evolutions with low probabilities. The probability of an attack strategy is defined based on the complexity of actions and resources required by an attack, and are based on historical data regarding the occurrence of attacks.

A metamathematical framework for the selection of the optimal set of countermeasures based on minimal sets and a partial ordering among subsets of countermeasures accompanies the approach proposed.

Software tools supporting (1) the design of evolution graphs, (2) the pruning of a graph (the removal of the nodes and arches selected according to the strategy described in the paper) and (3) the choice of countermeasures are developed to facilitate and automate the approach proposed.

The application of the approach is demonstrated on generic graphs which may illustrate a water distribution, a pipeline system or a sales devices data collection infrastructure.

4.11. *Network Security Risk Model (NSRM)*, 2009 **Error! Reference source not found.**

The Network Security Risk Model (NSRM) is introduced in **Error! Reference source not found.** The NSRM is a directed graph representing an attack. In a graph, nodes depict the components of a system and edges denote linkages through which one component may influence another. The purpose of the model is to assist with the selection of risk management controls by providing a measure of risk and by calculating the measure for a baseline and for a security enhanced versions of a system.

The application of the model is demonstrated on a simplified crude oil pipeline pump station controlled by a SCADA system which is a part of a larger process control network.

The NSRM comprises eight steps:

1. Identify risk metrics specific to a system. In the example presented in **Error! Reference source not found.**, risk is measured in terms of the gallons of crude oil lost flow per day. Two metrics, expected and extreme event loss production, are

examined.

2. Decompose a controlled infrastructure in a hierarchical model.
3. Characterise process failure modes and effects using Adaptive Multi-Player Hierarchical Holographic Modelling (AMP-HHM) framework **Error! Reference source not found.**, where in order to get a broader view a conflict is examined from the perspectives of both opposing sides.
4. Specify model processes and process disruption modes. Process specification is developed from a hierarchical model of a system;
5. Construct an attack scenario using HHM and AMP-HHM. Each attack scenario is characterised by attacker objectives, attacker type and the points of access.
6. Characterise network security structure Level and Barrier Diagram (ALBD) **Error! Reference source not found.** which covers success levels, barriers with OR and AND junctions.
7. Decompose the control network via decomposing the resulting ALBD into network components and linkages between them.
8. Define process disruption modes and resource requirements in terms of component access for each attack scenario.

Based on the return, the optimal attackers policy is identified showing which components of a system and in what order an attacker may attempt to compromise. A loss of crude oil for a baseline systems and the probability of the success of an attack are calculated. Next, the same parameters are estimated for a security-enhanced versions of the system. The analysis of the trade-offs between risk metrics for each security-enhanced version of the system and the cost of the corresponding security solutions allows the identification of the optimal security strategy and helps with security budgeting.

In **Error! Reference source not found.**, a methodology for calculating all parameters of the system is provided. It is noted also that due to the lack of statistical data and due to the specifics of individual systems, experts must be involved in the estimation of parameters involved in the calculation.

4.12. *Attack Countermeasure Tree*, 2010 **Error! Reference source not found.**

In **Error! Reference source not found.**, the risk assessment method based on Attack Countermeasure Tree (ACT), which enriches a widely used in risk assessment concept of an attack tree with information about security countermeasures, is introduced. There are three types of events in an ACT: attack event, detection event and mitigation event. An ACT may be augmented with the cost of an attack and the amount of security investment. The cost of an attack is the cost of the consequences of events leading to an attack with the minimal cost and is restricted by the budget of an attacker.

Attack scenarios may be produced from an ACT, as well as information extracted enabling qualitative and probabilistic security and risk assessment. Qualitative analysis allows the identification of the minimal combination of attack events as in any attack tree. The probability of an attack may be calculated based on the probabilities of single attack events. Formulas for calculating return of investment and return of attack are also suggested.

An ACT may be used to find the minimum set of defence mechanisms which includes at least one defence mechanism from each attack path. If more than one of such sets are found then other parameters (e.g. the cost of a set or the probability of an attack)

may be used to choose the optimal set.

The use of an ACT is demonstrated on a case study of a SCADA attack. The analysis in **Error! Reference source not found.** was performed using a software tool SHARPE (Symbolic Hierarchical Automated Reliability and Performance Evaluator), “*a general hierarchical modeling tool that analyzes stochastic models of reliability, availability, performance, and performability*” **Error! Reference source not found.** The optimisation was performed in MATLAB.

4.13. *Adversary-Driven State-Based System Security Evaluation,* 2010 **Error! Reference source not found.**

In **Error! Reference source not found.**, the ADversary View Security Evaluation (ADVISE) method is proposed. It enriches an attack graph with the characteristics of an adversary. The purpose of the method is to simulate an attack on a system, identify the most likely attack path and to calculate the probability of the success of an attack using an executable state-based security model of a system.

The ADVISE method recommends to follow three steps in order to receive an answer to a security question: (1) characterise adversaries and system, and specify security metrics; (2) developed an executable attack graph describing possible attacks; and (3) execute the graph to produce an answer.

A security model of a system, an attack execution graph, includes security-relevant system characteristics presented as a set of attack steps and the characteristics of an adversary. An attack step, an example of which is depicted in Figure 3, is characterised by attack precondition, execution time, cost, a set of outcomes, outcome distribution, detection distribution, payoff and state variable updates. An adversary is characterised by two system-independent characteristics (attack preference weight and attack skill level) and by three system-dependent characteristics (attack goal, system access and system knowledge).

In 2011, in the follow up paper **Error! Reference source not found.** a software tool that automates the ADVISE method was presented. The tool, which is built upon the existing modelling tool Möbius **Error! Reference source not found.**, automates input of system and adversary data, and the generation of executable models.

In **Error! Reference source not found.**, another case study is presented based on the comparison of two generic SCADA architectures described in NIST SP 800-82 **Error! Reference source not found.** attacked by four types of adversaries.

4.14. *Risk-Assessment Model for Cyber Attacks,* 2010 **Error! Reference source not found.**

Another risk-assessment model for cyber attacks on Information Systems is introduced in **Error! Reference source not found.** and its application is demonstrated on a test SCADA system of a chemical plant. The model may be used for risk assessment, cost-benefit analysis supporting the acquisition of IT components, and for the calculation of insurance premium by insurance companies.

Based on the literature review and their research, the authors of the paper enumerate seven possible attack types (replay capture, spoofing, denial of service, control message modification, write to master terminal unit, write to remote terminal unit and remote terminal unit response alteration) and specify six types of loss an attack may

cause (control-loss, product-loss, staff-time loss, equipment damage, and prevention) along with the probability of type of loss for each type of attack.

A loss caused by an attack in **Error! Reference source not found.** depends on the type of an attack and other losses as estimated by chemical plant experts. The paper presents a formula for calculating a loss of each type. The prevention cost, for example, is calculated as a product of the cost of the upgrade of IT components resistant to a specific type of attack and the probability of prevention loss for this attack type. Ultimately, a total estimated revenue loss from all types of cyber attacks may be calculated using the model proposed.

It is mentioned that a tool was developed to automate the loss estimation process suggested, but no details regarding the tool is provided.

4.15. Cybersecurity for Critical Infrastructures: Attack and Defense Modelling, 2010 **Error! Reference source not found.**

A SCADA security framework RAIM, which consists of four parts (Real-time monitoring, Anomaly detection, Impact analysis and Mitigation strategies) is introduced in **Error! Reference source not found.**

The real-time monitoring and anomaly detection modules of the framework are based on the continuous monitoring of system logs and are needed to collect data for the subsequent impact analysis. Impact analysis aims to examine intrusion behaviours and a possible impact of a cyber attack on a SCADA system and consists of four steps: (1) capturing system configuration in a cybernet; (2) power flow simulation; (3) vulnerability index calculation; and (4) security improvement.

Impact analysis is based on an attack tree where a cyber security vulnerability index shows the likelihood of a leaf of an attack tree being compromised, the likelihood of a specific intrusion scenario or of the overall attack. The indices are calculated based on historical data regarding intrusions, and information about security countermeasures and password policies. The leaf vulnerability index depends on port auditing and password strength.

The application of the framework is demonstrated on a test subnet of electric power control network.

4.16. Digraph Model for Risk Identification and Management in SCADA Systems, 2011 **Error! Reference source not found.**

A digraph model of a SCADA system for a chemical distillation column of a laboratory scale is presented in **Error! Reference source not found.** The model provides a formal representation of the structure and behaviour of a SCADA system and may be exploited for risk impact assessment and fault diagnosis.

The vertexes of the graph are the components of a SCADA system and a directed edge exist between two vertexes if a security risk at an initial vertex may affect security of a terminal vertex. The reachability matrix of a graph and its partitioning may be used to separate the components that are more likely to be impacted from those that are less likely to be impacted if the component represented by the initial vertex of a digraph is found at risk. For fault diagnosis a digraph is used in a deductive manner in a way similar to fault trees. It is used to identify the sources of a fault when a fault is observed in one of the components. The ancestors of all faulty components form the set of potential fault sources. The set is then reduced to one source which is common to all faulty

components. The use of digraph for fault diagnoses is exemplified on the scenario where a hacker penetrates a corporate network and then injects a SCADA DNP3 traffic with a malicious code.

4.17. *Risk Assessment, Detection, and Response,*

2011 **Error! Reference source not found.**

A risk assessment method for sensor networks accompanied by attack detection and automatic response modules are presented in **Error! Reference source not found.**

In **Error! Reference source not found.**, the standard formula for calculating risk as an average loss is accepted and interpreted in the context of a sensor network:

$$R_{\mu} = \sum_i L_i p_i \quad (4)$$

where p_i - the probability of an attacker compromising sensor i and is accepted to be the same for all sensors and L_i - a loss resulting from the compromise.

The following attack model is proposed which may reflect integrity and DoS attacks:

$$\tilde{y}_i(k) = \begin{cases} y_i(k), & \text{for } k \notin \mathcal{K}_a \\ a_i(k), & \text{for } k \in \mathcal{K}_a, a_i(k) \in \mathcal{Y}_a \end{cases} \quad (5)$$

where $\tilde{y}_i(k)$ - a measurement received by the controller at time k ; $y_i(k)$ - an actual measurement; $a_i(k)$ - a measurement under attack; and \mathcal{K}_a - the duration of an attack.

For detecting anomaly, a linear model as an approximation of the behaviour of a physical system is developed. Then, anomaly is detected using a non-parametric cumulative sum statistic. When anomaly is detected, an automated response to an attack is fired while awaiting human actions.

The experiments were run to simulate cyber attacks on a chemical reactor implemented as a Tennessee-Eastman process control system model presented in **Error! Reference source not found.** The experiments demonstrated that the risk assessment model proposed helps to establish which type of attack and which sensor in a network must be given a priority in a security budget.

4.18. *Cyber Security Risk Assessment in Nuclear Power Plants,*

2012 **Error! Reference source not found.**

A cyber security risk assessment methodology that may be exploited in the process of the design of instrumentation and control systems in nuclear power plants is suggested in **Error! Reference source not found.**

The methodology outlines six steps that must be undertaken in order to conduct cyber security risk assessment during the system and component design, and equipment supply stages:

1. System identification and cyber security modelling,
2. Asset and impact analysis,
3. Threat analysis,
4. Vulnerability analysis,
5. Security control design, and
6. Penetration test.

The paper describes the activities that must be undertaken during each step by summarising the relevant NIST standards. Possible attack scenarios are listed to be used

in threat analysis. As for vulnerability analysis, it is recommended to use an existing lists of vulnerabilities and adapt them to the specifics of a system under analysis. Security controls may be adopted from relevant NIST standards (e.g. NIST SP

800-82 **Error! Reference source not found.**). Finally, security control design must be validated by means of vulnerability scans and penetration tests.

4.19. *Boolean logic Driven Markov Processes,*

2012 **Error! Reference source not found.**

The Boolean logic Driven Markov Processes (BDMP) modelling approach is described in **Error! Reference source not found.**

The BDMP formalism, which combines fault trees with Markov processes, facilitates the modelling of an attack on a system. Qualitative and quantitative outcome useful for risk assessment may be produced from a BDMP model.

The BDMP formalism uses the following modelling objects: (1) leaves for attack modelling, namely Attacker Action, Timed Security Event and Instantaneous Security Event; (2) gates such as AND and OR, and several specific gates; and (3) links including classical logic links and two specific links, Trigger Link and Before Link. An example of the STUXNET attack model rendered using the BDPM modelling approach is presented in **Error! Reference source not found.** A leaf of a BDPM model is characterised by success rate and probability. All attack paths may be identified and ordered by their probabilities or by effect on attack success.

The quantitative analysis of the STUXNET BDPM model in **Error! Reference source not found.** was performed using modelling tool

KB3 **Error! Reference source not found.** The probabilities and success rates of the leaves of the model were quantified by the authors of the paper “*based on [their] own estimation and writings by security consultants*” **Error! Reference source not found.**

4.20. *A CORAS-based Risk Assessment for SCADA,*

2012 **Error! Reference source not found.**

CORAS [49, 50] is a model-based risk assessment method designed for security critical systems. It is based on ISO/IEC 31000. CORAS is designed for “*security-critical systems in general, but puts particular emphasis on IT security*” **Error! Reference source not found.** CORAS covers the entire risk

management process and heavily uses models at many stages of risk management.

There is a large number of publications related to CORAS². In this paper, we analyse only the publication related to the application of CORAS in the context of a SCADA system, namely **Error! Reference source not found.**

In **Error! Reference source not found.**, CORAS is used for the risk analysis of a SCADA system. First, assets and their levels of importance are identified. Then, threats and vulnerabilities are listed. Finally, using the CORAS modelling language a set of threat diagrams is developed. The threat diagrams presented in the paper were created as a result of a brainstorming session in which security and risk experts participated along with system stakeholders.

The paper reports only preliminary results of a research project and outlines an

²http://coras.sourceforge.net/online_documentation.html

extensive future work. In the main, **Error! Reference source not found.** demonstrates that the CORAS modelling language is useful for threat modelling in the context of a SCADA system.

4.21. *A PMU-based Risk Assessment Framework for Power Control Systems, 2013* **Error! Reference source not found.**

In **Error! Reference source not found.**, a Phasor Measurement Unit (PMU)-based risk assessment framework for SCADA systems of power grids is introduced. The application of the framework is demonstrated using a simulation on the IEEE 10 Generator 39 Bus System.

The steps of the framework as described below. First, the configuration of a system is identified. Next, vulnerabilities within the system are identified and quantified using the Duality Element Relative Fuzzy Evaluation Method (DERFEM). Then, an attack graph is designed and used in order to find intrusion scenarios, the probabilities of which are also calculated.

In addition, the paper presents System Stability Monitoring and Response System (SSMARS). SSMARS is an on-line scheme based on PMU data. It monitors the impact of adversary events on a power system in real time and induces control actions to control voltage when needed.

4.22. *Improved Risk Assessment Method for SCADA Information Security, 2014* **Error! Reference source not found.**

In **Error! Reference source not found.**, a modification of a traditional method for calculating the effectiveness of intrusion, detection and prevention systems in terms of averting a specific class of attacks on a system is presented. The purpose of the method is to “allow the determination of the optimum level of security investment and definition of different levels of acceptable risk”. The method, according to its authors, enables a more precise calculation of loss expectancy than any other method. This is achieved by taking into account the strength of an attack and its effect on the system performance, which is measured using weighing factors.

The following formula is introduced in **Error! Reference source not found.** for calculating Annual Loss Expectancy (ALE):

$$ALE = W_A \prod_{i=1}^N W_i \left(\sum_{j=1}^M DL_j \right) \times ARO \quad (6)$$

where W_A - weighting factor, which scales maximum direct losses depending on the strength of attack; N - the number of conditions contributing to indirect losses; W - indirect costs resulting from a condition; M - the number of loss types; and ARO - the annual rate of the occurrence of an attack, which is defined based on the analysis of historical data.

Return on Security Investment (ROSI) is then calculated as follows:

$$ROSI = (ALE \times \% RiskMitigated - C_s) / C_s \quad (7)$$

where C_s is the cost of implemented security controls.

The application of the method is demonstrated on a case study of a run-off-river hydro-power plant.

4.23. *Cyber-Security Analysis of Smart Grid SCADA Systems with Game Models, 2014* **Error! Reference source not found.**

The application of game theory to a cyber security analysis of a smart grid SCADA system is discussed in **Error! Reference source not found.**. The interaction between an attacker and a defender (a SCADA system administrator) is modelled as a two-player, non-cooperative, sequential, perfect information and non-zero sum game. The approach is demonstrated on a case study of the sensor network of a smart grid SCADA system.

Within the approach, a game tree is developed and populated with players' payoffs. In order to develop a game tree, first, the following possible actions of an attacker are defined: a_s - Sybil attack, an attacker deploys a malicious (Sybil) sensor device, which acts as a legitimate sensor; a_{NC} - node compromise, a_e - eavesdropping; a_{DI} - data injection; and a_{NIL} - no attack action. Then, the possible defender response modes are defined as r_c - cut-off energy to a sensor, r_a - alert MTU, and r_m - maintain correct data and valid nodes.

The following formula for calculating an impact of an action a is presented in **Error! Reference source not found.**:

$$Impact(a) = w_c C(a) + w_i I(a) + w_a A(a) \quad (8)$$

where w_c, w_i , and w_a are the weights of confidentiality, integrity and availability respectively and $C(a)$, $I(a)$ and $A(a)$ are the impacts of action a on confidentiality, integrity and availability respectively. The parameters in this formula are quantified based on expert opinion and historical data. The payoff of a player at a current decision node is calculated as a sum of his previous payoff at the parent node and the current payoff, which is a function of the impact of the current action on the player. Game theory analysis in **Error! Reference source not found.** helps to identify a payoff of an attacker and defender at each step and to establish the strategies with the best payoff for both players.

4.24. *Quantitative Methodology to Assess Cyber Security Risk of SCADA Systems, 2014* **Error! Reference source not found.**

A methodology for quantitative assessment of cyber security risk in SCADA systems based on the optimal power flow and power flow tracing is introduced in **Error! Reference source not found.**.

The fifteen types of threats and the four components of a SCADA system (EMS server, a SCADA server, RTU and communication network) are distinguished in **Error! Reference source not found.**. For the quantification of vulnerabilities, first, the relevance of each threat to each component is defined. Then, a vulnerability index is assigned to each component of a system. The vulnerability index of a component is based on historical data, where available, and on the security characteristics of the component. For the quantification of threats, a normalised weighted index is assigned to each type of threat for each component of a SCADA system. It is based on the applicability of the threat to the component, the vulnerability index of the component and the damage capacity of the component. The asset value is calculated based on the outage cost.

The optimal power flow is estimated as a minimal power generation cost for all generators under the restrictions on generators and line capacities. The power flow tracing method, which is based on the graph theory, is then used to examine the interdependencies between generators and load terminals in order to calculate outage cost

for each component of a SCADA system.

Finally, risk is calculated in monetary terms as a product of the probabilities of a threat and vulnerability, and of the cost of an asset.

5. Summary Analysis and Key Findings

5.1. Descriptive Statistics

The list of the risk assessment methods described in the previous section is summarised in Table 1. In Table 1, *country* is the country of the first author of the paper and *citations* is the number of citations of the paper according to Google Scholar Citation Index as on 12 January 2015.

The number of papers covering risk assessment in SCADA produced between 2004 and 2014 vary between 0 and 4 per year (Figure 4). No noticeable increase in the number of papers over time is encountered. Among the papers analysed, the research from the following countries France, Canada, China, Australia, Serbia, Ireland and Italy is represented by one paper each. Two papers originate from Korea, while the majority (15 papers) are produced by researchers from the USA.

The largest number of citations (104) is acquired by **Error! Reference source not found.** published in 2011. It is worth noting here that **Error! Reference source not found.** covers the scope broader than risk assessment and describes also modules for attack detection and automated response to an attack. The second most cited paper among analysed, with 87 citations, is **Error! Reference source not found.** which is published in 2010 and which introduces the four component (real-time monitoring, anomaly detection, impact analysis and mitigation strategies) security framework for SCADA systems. The third most cited paper, with 85 citations, is **Error! Reference source not found.** which is published in 2004 and describes the use of attack trees for assessing vulnerabilities in SCADA systems.

5.2. Categorisation of the Methods

Most often, risk assessment methods in general are classified into qualitative and quantitative [30, 31, 32], with semi-quantitative methods being distinguished in some publications [32, 33]. While qualitative methods use a subjective classification of risk (e.g. low-medium-high), quantitative methods strive to measure risk numerically. The majority of quantitative methods are probabilistic. The difficulties of the quantitative measurement of security which hold in the risk quantification context also are discussed in **Error! Reference source not found.**

Alternatively, risk assessment methods are classified into traditional assessments and baseline controls **Error! Reference source not found.**

In **Error! Reference source not found.**, a new classification scheme for risk assessment methods is suggested. It separates methods into nine categories according to the approach used, and the level of the involvement of a risk expert and system owner.

Risk assessment methods based on graphs are widespread. Tree-based risk assessment methods (e.g. fault tree, attack tree, event tree, vulnerability tree and various combinations of the above) as well as other risk assessment methods based on directed graphs fall under the category of probabilistic methods. Tree-based methods are similar in their logic and aim to define the probability of the top event or its

reliability **Error! Reference source not found..** What constitutes the major difference between various tree-based methods is the top event. In [7, 13, 31, 36], among probabilistic tree-based methods for SCADA systems inductive and deductive methods are distinguished. Inductive methods (e.g. event tree) trace from possible causes to undesired events as opposed to deductive methods (e.g. fault and attack trees), which trace from undesired events to possible causes **Error! Reference source not found..** Inductive methods are also referred to as forward search techniques, while deductive methods are referred to as backward search techniques **Error! Reference source not found..**

As pointed out in [6, 7], risk assessment methods as applied to SCADA systems are difficult to categorise. Based on the analysis presented in this paper, we suggest an intuitive categorisation for the methods examined. This classification scheme is generic and we foresee that it may be applied to other domains.

First, the methods examined may be categorised by the level of detail and coverage as follows:

- *Guidelines* - outline a set of steps for a user to follow either assuming that the user knows how to perform each step or, in better cases, providing references to specific methods that may be exploited. An exhaustive description of activities within each step is absent. Guidelines strive to cover the majority of the stages of the risk management process. The coverage of the stages by guidelines is broad, while the level of detail provided is low.
- *Activity-specific methods* - focus on and in depth examine a specific activity performed at a certain stage of the risk management process. The level of detail here is high, while the coverage in terms of the stages of the risk management process is narrow.
- *Elaborated guidelines* - are the combinations of the two categories listed above. Elaborated guidelines provide a coarse outline of many or even all stages of the risk management process and concentrate particularly on one or more specific activities within the process. The coverage of the risk management process stages here is broad and the level of detail provided is high.

The categorisation of the methods analysed into guidelines, activity-specific methods and elaborated guidelines is summarised in Table 2, which shows that the majority of the methods examined fall under the category of activity-specific methods.

Second, the risk assessment methods examined may be split into:

- *Formula-based methods* - these methods are based on mathematical models of risk. A formula-based method consists of a set of formulas to calculate risk or impact. These methods do not use any models to support risk assessment, but represent supporting information in a tabular or textual form.
- *Model-based methods* - in these methods risk analysis is based on a *graphical* model. These methods, in the majority of cases, are supported by mathematical models as well to enable qualitative and typically probabilistic analysis. Among model-based methods one may separate graph-based methods and methods based on other types of models (e.g. HHM).

Table 4 shows the categorisation of the papers examined into formula- and model-based methods. The majority of the methods are based on graphs or their multiple variations as Table 4 hints at. Attack trees are used in the large number of proposals.

Many attack-tree-based methods either enrich an attack tree with additional data or combine it with the models of other types (Table 4).

Three of the papers examined, namely [61, 75, 57], we were not able to assign to either formula- or model-based category since the papers are guidelines, and the specific methods of analysis within these guidelines must be chosen by users.

As Table 4 also shows that among the model-based methods, the vast majority are attack- or failure-oriented, while only three methods [11, 23, 63] are goal-oriented. More precisely, **Error! Reference source not found.** exploits dual approach, while infrastructure hypergraph may be attributed to the goal-oriented approach, evolution graph belongs to the attack-oriented approach. The goal-oriented approach focuses on positive outcomes and bring together the elements that an organisation's success **Error! Reference source not found.** as opposed to failure-oriented approach that concentrates around the identification of all possible types of attack and failure modes.

Traditionally, we also split the risk assessment methods examined into qualitative and quantitative as summarised in Table 3. More than a half of the methods examined are probabilistic. Three methods are quantitative, but do not use the notion of probability in their quantification of risk. Five out of the methods examined are qualitative.

5.3. Probabilistic Methods

Table 3 indicates that Probabilistic Risk Assessment (PRA) methods are widely used in risk assessment of SCADA systems. However, PRA methods suffer from a range of disadvantages [6, 11, 89]:

- The estimation of risk is never complete in the mathematical sense. The reader may want to return to Formula 1, where a complete set of undesired events is never known.
- No way is provided to deal with hitherto unknown vulnerabilities, attacks or failure modes.
- Continuous revision is required. In Formula 1, a revision is needed in order to keep a set of undesired events as complete as possible reflecting the rapidly evolving cyber security domain, or, turning to Formula 2, to keep the set of known vulnerabilities and threats up-to-date. In 1979, it was stated: *"It is conceptually impossible to be complete in a mathematical sense in the construction of event-trees and fault-trees; what matters is the approach to completeness and the ability to demonstrate with reasonable assurance that only small contributions are omitted. This inherent limitation means that any calculation using this methodology is always subject to revision and to doubt as to its completeness"* **Error! Reference source not found..** Attack and vulnerability trees, which belong to PRA methods, usually concentrate on a specific type of attack and at best attempt to cover *"all known threats and vulnerabilities in an infrastructure"* [31, p.484], ignoring unknown threats.

In **Error! Reference source not found.**, it is declared that *"in very large and complex situations the exhaustive computation of all possible attacks is often impossible or simply not practical."*

- Context establishment, upon which risk identification draws, is not given direct attention (Section 5.7).
- Methods rely either on historical system data, which is difficult to access, or on subjective data (Section 5.4). The availability of objective data for analysis limits

the applicability of many PRA methods. In **Error! Reference source not found.**, it is recommended to *“avoid use of the probabilistic risk analysis methodology for the determination of absolute risk probabilities for subsystems unless an adequate data base exists and it is possible to quantify the uncertainties.”*

- Indirect, non-linear and feedback relationships that characterise many incidents in SCADA systems are not accounted for.
- Numerous simplifying assumptions, which do not always hold in real life, are made. For example, a few of the assumptions encountered by this analysis are *“adversaries are like managers of multinational corporations who make rational choices investments and expected returns”* **Error! Reference source not found.**, *“the vulnerabilities of each component C are known”* **Error! Reference source not found.**, perfect information of an attacker and a system administrator when *“both players know what has happened to the system so far before making their decision on the next move”* **Error! Reference source not found.** and *“the defender will not take any action to defend the system unless an attack action occurs”* **Error! Reference source not found.**. The examples of other assumptions are the independence of security events, the stationarity of a system over time or similarities with other systems, the use of the aggregation of security numbers related to the different components of a system overlooking mutual interdependencies **Error! Reference source not found.**. A method based on wrong assumptions may highly likely produce incorrect results.

- Methods do not effectively cope with risks with low probabilities, but extreme, catastrophic consequences **Error! Reference source not found.**. For predicting catastrophic events such as for example 9/11, Fukushima and Chernobyl frequency-based statistical methods on which PRA methods rely have little value [89, 93].

Despite their drawbacks PRA methods are popular among the researchers and practitioners predominantly because they provide a convenient numeric estimation of risk which assists security decision-makers with the understanding of the security posture of an organisation and with the allocation of security funds.

5.4. Sources of Probabilistic Data

Table 5 shows that in the methods examined probabilities used for the calculation of risk or impact are derived based on historical data (e.g. incident logs as in **Error! Reference source not found.**), expert judgement or both. In five methods, we were not able to find any indication of where probabilistic data come from.

PRA methods typically use probabilistic data to measure at least one or several metrics, e.g. vulnerability existence, vulnerability severity, attack frequency, loss occurrence, detection and mitigation rates, attack step success and overall attack success to name just a few. Hence, the success of a PRA method strongly depends on the quality of estimated probabilities, which ideally should originate from objective empirical rather than hypothetical data. Objective data in this instance is data received from statistical sampling, historical records or experimentation **Error! Reference source not found.**

The authors of the methods examined point out that data required for the effective estimation of risk is rarely available [18, 83] and, therefore, research often has to rely on artificial data **Error! Reference source not found.**. Objective data may often be unavailable due to various reasons: hardware and software specifics, legacy and

confidentiality. Undoubtedly, this issue hinders the validation of the methods, and diminishes the trustworthiness of risk assessment results.

In **Error! Reference source not found.**, the authors consciously avoid the use of probabilistic data, but characterise security by median loss and maximum loss. However, this approach is based on the assumption that it is possible to identify a complete set of all failure and attack modes. This assumption is open to argument.

In the method examined where expert opinion is used little or no detail is provided as to how the opinion was captured and analysed. Ultimately, this is a crucial point of any expert opinion-based method since the correctness of risk estimation is founded in the precision of the probabilities involved in the calculation.

5.5. *Domain and Aim*

More meticulous overview of the methods examined is summarised in Table 6, where the domain, aim and evaluation route are outlined for each method.

The risk assessment methods are developed for and applied to a range of domains including power grids, chemical plants, pump systems and rail road sector. Table 6 shows that eleven out of twenty four proposals deal with SCADA systems in power sector considering smart grids, hydro power and nuclear power plants. Four proposals [61, 63, 67, 78] do not mention any specific sector, but discuss SCADA systems in general.

The methods examined vary significantly in terms of their aims because their cover different stages of the risk management process or different activities within the same stage. While one method **Error! Reference source not found.** aims to list and discuss risk assessment activities to be undertaken at the system design stage, four methods [11, 57, 59, 72] target to identify vulnerabilities and/or to quantify the level of vulnerability of a system. The method presented in **Error! Reference source not found.** strives to identify sources of risk. The declared aim of three methods [31, 63, 67] is the assistance with the selection of an optimal set of countermeasures.

5.6. *Evaluation*

As Table 6 indicates the vast majority of methods are evaluated by means of a single case study or example. A case study or an example is typically based on a generic and simplified model of a system or on a testbed. In some instances, a method is not demonstrated in full, only some activities within the method are dealt with in a case study (e.g. **Error! Reference source not found.**) In three proposals [23, 57, 59] no discussion of a method evaluation was found. The application of a method to a real world system is declared as future work in several proposals (e.g. **Error! Reference source not found.**). Only in two papers, namely [18, 71], it is explicitly mentioned that the method was applied to a real system. In **Error! Reference source not found.**, the validity of an attack tree is evaluated by energy sector operators and the feasibility of attacks is tested in a laboratory setting. In **Error! Reference source not found.**, the guideline aiming at protection of SCADA systems from the threat of cyber-terrorism within Australia is evaluated by a focus group of five SCADA system consultants.

Unsurprisingly, the analysis of the risk assessment methods for SCADA systems in terms of their evaluation leads to a conclusion that it is easier to propose a method than to evaluate it in a sustainable rigorous manner. The methods are rarely, apart from a few exceptions, discussed with industry experts (Table 6). Since the methods are not applied to real systems, the validity or practicality of the results rendered by a method are also

not evaluated by industry experts.

In few cases, where a method is applied to a real system, a system is accessed only once and is not revisited again for retesting or regarding the feedback on the usefulness and effectiveness of the method.

For the qualitative methods it is not discussed whether the outcome produced by the method gives a sufficiently accurate description of risk. The same is true for quantitative methods. In **Error! Reference source not found.**, the method is said to “enable a coarse quantification of the attack success probability”, but it is not validated whether the quantification suggested is accurate enough to back up security decisions.

In the methods examined, the formulas provided for the quantification of risk, impact or attack probabilities are typically not proved in a mathematical sense. The proof is often limited to the statements like in **Error! Reference source not found.** saying that the formulas suggested have “intuitive meaning for the analysts, testers, and control system users” and are “clear, reasonably intuitive, and sufficiently well-defined to guide the analysis of the proposed method”. Unfortunately, what is intuitive and clear vary from person to person and is very subjective.

5.7. Stages of Risk Management

The process of risk management, as it is adopted in ISO 31000:2009(E) **Error! Reference source not found.** and ISO/IEC 27005:2011 **Error! Reference source not found.**, is depicted in Figure 5.

ISO 31000:2009(E) **Error! Reference source not found.** provides the following definitions for risk management and risk assessment:

Risk management - “coordinated activities to direct and control an organisation with regard to risk” [21, Def. 2.2];

Risk assessment - “overall process of risk identification, risk analysis and risk evaluation” [21, Def. 2.2], where **risk identification** is the “process of finding, recognizing and describing risks” [21, Def. 2.15], **risk analysis** is the “process to comprehend the nature of risk and to determine the level of risk” [21, Def. 2.21] and **risk evaluation** is the “process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable” [21, Def. 2.24].

Table 7 shows which stages of the risk management process are addressed by each method. The stages and their definitions are adopted as outlined in ISO 31000:2009(E) **Error! Reference source not found.** and ISO/IEC 27005:2011 **Error! Reference source not found.**

In Table 7 the cell is left empty if the stage is not addressed by a method; ● means that the stage is addressed in detail; and ◐ denotes that the stage is partially addressed (i.e. it is briefly outlined, but no detailed recommendations on the execution of the activities associated with the stage are provided). The last column of Table 7 describes the metrics analysed or measured by the methods.

According to Table 7, the vast majority of methods concentrates on the risk identification and risk analysis stages of the risk management process, while other stages receive noticeably less attention.

Little or no attention is devoted to the risk evaluation stage. Quantitative risk

metrics are often hard to be judged on an absolute scale and require a basis for relative comparison to support security decision-making. We did not encounter an explicit process of comparing the results of risk analysis with risk criteria in the proposals. In the majority of the papers also no discussion was found regarding whether resulting risk metrics, such as vulnerability index or impact are acceptable or tolerable. There are though several proposals [18, 31, 64, 69], which we mark with **D** regarding risk evaluation in Table 7, where the comparison of risk metrics is performed between different security configurations of a system.

It is hard to overestimate the importance of the context establishment stage. Risk management decisions must be well-informed and based on an in-depth knowledge of a system and its environment. A complete set of risks to a system may not be identified without an understanding of system configuration, interactions with other systems, stakeholders' goals, rights and responsibilities, and human-machine interactions. During the context establishment stage an organisation examines its structure, current security posture, specifies security goals and security strategy, investigates possible external influences **Error! Reference source not found.**. This stage facilitates the scoping and focusing of the process, e.g. the identification of critical assets calling for larger security investment.

Our analysis indicates that the quantitative probabilistic methods in general do not concentrate on the context establishment stage. In the majority of the papers where context establishment is addressed it is limited to the understanding of a system or network configuration. Consequently, only risks associated with the ICT components of a SCADA system are taken into account by a risk assessment method while overlooking a large number of risks arising from non-technical aspects.

Among all methods examined only **Error! Reference source not found.** is exclusively dedicated to the understanding of a SCADA system. The holographic model of a SCADA system presented in **Error! Reference source not found.** addresses an extensive range of technical and non-technical subtopics relevant to various aspects of the system. These subtopics are ultimately the sources of risk to a SCADA system.

5.8. Key Concepts and Impact Measurement

The following key concepts of risk management are widely acknowledged in the literature: *system (asset)*, *vulnerability*, *threat*, *impact (consequence)* and *security control (countermeasure)* [13, 17, 33, 34, 78]. Table 8 shows which key concepts of the risk management domain are addressed by the methods examined. The term *system* or *asset* is used here in a wider sense and refers to people, knowledge, the structure of the system and its organisation rather than purely to the technical equipment of a SCADA system.

Table 8 confirms the conclusions drawn in the previous section about insufficient attention to context establishment by indicating that only 9 methods address the *system/asset* concept. Attacks are dealt with by 18 methods, while risk impact is measured in 15 proposals. A fewer proposals address vulnerabilities and countermeasures, 14 and 12 respectively. A minute description of the concepts analysed or measured by the methods could be found in the last column of Table 7.

One of the major requirements to a risk assessment method is to produce simple key security indicators which would enable senior management and security experts to take well-informed security decisions without getting lost in technical detail **Error! Reference source not found.**. Therefore, the choice of key indicators and

their metrics is important.

The analysis confirms that impact or consequences are typically measured in monetary terms. In **Error! Reference source not found.**, the impact is measured in monetary terms plus a number of human lives. In [72, 80], numeric indices are proposed. Several methods point out that risk or impact indicators (and, consequently, their measurement) must be chosen in collaboration with system managers and must be meaningful in the context of a specific organisation or domain.

5.9. *Tool Support*

In the vast majority of the proposals examined (17 out of 24) no software prototype or tool supporting the method is discussed. In several papers the development of a software prototype is outlined as a subject of future work (e.g. [18, 68]).

Out of twenty four papers examined a software prototype or tool supporting the method is discussed only in seven papers, namely [63, 67, 69, 71, 72, 73, 76]. In four out of these proposals, supporting software is based on the existing tools.

In **Error! Reference source not found.**, the authors use the existing tools SHARPE and MATLAB. In **Error! Reference source not found.**, the prototype is based on the existing modelling tool Möbius. In **Error! Reference source not found.**, the tool builds upon MATLAB and uses FORTRAN. In **Error! Reference source not found.**, another existing tool, KB3, automates risk assessment method proposed.

Even in the small number of the papers where tool support is discussed, the information regarding a tool is extremely scarce and most often is simply limited to the statement that a tool was developed (e.g. in [72, 71]). Neither the architecture of a tool nor user interface are demonstrated.

6. **Research Challenges**

6.1. *Dealing with Fragmentation*

We encountered a certain level of fragmentation in terms of addressing the stages of the risk management process. In particular, little attention is paid to the context establishment stage of the risk management process. Any risk assessment method would benefit from an in-depth understanding of a SCADA system, its components and the interdependencies between them, and external factors affecting it. The methods often either try to cover many stages of the process at the expense of the level of detail or focus on one stage providing no instructions regarding the other stages. There is clearly a need for a comprehensive method which would cover all stages of the risk management process and deal with all key risk management concepts.

Little attention is received by the context establishment stage. It is typically assumed that a user of a risk assessment system knows the system and its interdependencies well. However, due to the inherent complexity of SCADA systems such assumption is hardly always true. Also when establishing the context at the initial stage of the risk management process often only the technical aspect of a SCADA system is addressed. In future, risk assessment methods may draw upon more definite account of the human factor, individual knowledge, personnel cyber security awareness, organisational cyber security culture and business processes.

6.2. *Overcoming Attack- or Failure-Oriented*

As a result of the concentration on threats and vulnerabilities during the risk management process, rather than on system itself the vast majority of the risk assessment

methods examined are failure-oriented (Table 4). Thus, “[u]nderstanding consequences and estimating likelihood from cause-related logic trees seem to be pre-requisites of any approach to analyzing risks in a system ... ” [94, p.5].

However, as noted earlier in the paper, it is not always feasible to envision *all* possible failure modes or attacks. We see the application of a goal-oriented approach to risk management **Error! Reference source not found.**, which would support risk management even in situations where a comprehensive list of failure modes or attack types may not be established, as one of the research challenges of the field. Approaching risk management from the positivist top-down perspective by identifying the elements and dependencies within a SCADA system that are required in order for a system to be operational, safe and secure offers a more solid understanding of a system and risk factors facing it as opposed to the failure-oriented perspective, which is by definition incomplete.

We believe that the use a goal-oriented dependency modelling approach **Error! Reference source not found.** in the context of SCADA systems offers multiple benefits including the overcoming failure-orientation. A dependency model focuses on positive outcomes and elements required by an organisation for smooth, safe and secure operation. A dependency model is developed by asking *What does the successful operation of a system depend upon?* rather than by examining system failure modes. It is not restricted to the boundaries of an organisation and it does not rely on historical data or on the completeness of the list of potential threats **Error! Reference source not found.** Linking to the previously outlined research challenge, a dependency model, which provides an insight into more fundamental aspects of a SCADA system, might support the context establishment stage as well as risk identification and assessment stages of the risk management process.

The development of a model of a SCADA system is an arduous task. Both qualitative and quantitative parameters of a dependency model of SCADA system are hard to establish and require reliable statistical data, and the involvement of SCADA and security experts. In future research, a method must be developed for updating the qualitative parameters of a dependency model of a SCADA system dynamically based on the information extracted from SCADA system models of other types, e.g. security-annotated business process models or UML class diagrams with security profiles. A method must automate the process of the creation and refreshing of a dependency model of a SCADA system by pulling together in a consistent way security related information from other models developed while designing a secure SCADA system.

6.3. Search for Reliable Sources of Data

Despite their drawbacks, PRA methods prevail over qualitative and quantitative non-probabilistic methods. One of the major obstacles for PRA methods is the lack of objective accurate data for the calculation of probabilities involved in risk assessment. In 2007, one of the studies on SCADA systems cyber security reported that “*accurate historical data on cyber impacts was badly lacking in the SCADA or process industries thus making accurate risk assessment extremely difficult*” **Error! Reference source not found.**

In order to deal with the absence of historical system data, several methods are discussed in the literature:

- The use SCADA test platforms to collect experimental data on threats and

vulnerabilities.

SCADA testbeds may fill up the lack of historical data by building up vulnerability and attack databases **Error! Reference source not found.** Controlled simulations on test platforms may help to collect statistics regarding vulnerability existence and severity, and attack success rates **Error! Reference source not found.** There is a range of SCADA testbeds developed by universities across the world [83, 87].

- The development of databases of security incidents in SCADA systems, A number of CNI, ICS and SCADA systems security databases exist, e.g. the RISI database **Error! Reference source not found.**, which is mentioned earlier in this section, and the Industrial Security Incident Database (ISID) **Error! Reference source not found.** Vulnerability databases accounting for SCADA systems are listed in **Error! Reference source not found.**
- The improvement of information sharing across research and industry, and Although information sharing initiatives exist (e.g. in order to facilitate information exchange, the European SCADA and Control Systems Information Exchange (EUROSCSIE) was established under the initiative of the CPNI **Error! Reference source not found.**) they do not typically involve researchers to the desirable degree. Many authors highlight that it is complicated or even virtually impossible for researchers to access realistic data regarding structure, threats and vulnerabilities of SCADA systems.
- Reliance on expert judgement and its formalisation.

In order to deal with the absence of historical data, some PRA methods rely on subjective data such as expert opinion (see Table 5). In some cases, expert opinion is more easily available and may even be more valuable than historical data.

However, risk assessment methods, which rely on expert opinion must devote more attention to techniques for capturing, formalising and ultimately turning into numeric values expert knowledge.

In 2007, in **Error! Reference source not found.** it was mentioned that a “*natural extension to PRA involves the use of fuzzy concepts, though this approach has not been published for use in SCADA system security risk assessment.*” In our analysis, we found only one method which uses fuzzy logic. In **Error! Reference source not found.**, the Duality Element Relative Fuzzy Evaluation Method (DERFEM) is exploited for quantifying the severity of vulnerabilities. Thus, while fuzzy methods seem promising in SCADA risk assessment their current application is limited.

6.4. Improving Validation of Risk Assessment Methods

According to **Error! Reference source not found.**, methods for quantifying security are in general weakly justified. Section 5.6 also confirms that there is room for improvement regarding the rigorous multi-aspect evaluation of risk assessment methods for SCADA systems.

Researchers rarely have a chance to evaluate their methods on real case studies and have to be satisfied with the demonstration of their methods on generic simplified examples. The testing of methods in practice with security, risk and SCADA experts, and with managers responsible for security decision-making is invaluable. It may help to evaluate whether a method accounts for the perspectives of multiple stakeholders and conveys cyber security risks in a clear form accessible to non-technical managerial staff

and SCADA experts lacking security background.

The general guidance on choosing an evaluation method (or a combination of them) could be found in **Error! Reference source not found.**, where methods are categorised into naturalistic (evaluation in real settings) and artificial (evaluation in laboratory settings, analytical evaluation, simulations etc.) as well as ex ante (evaluation of an uninstantiated artifact) and ex post (evaluation of an instantiated artifact). The authors of risk assessment methods may evaluate the process of risk assessment they propose or the outcome of it or both. As inspired by in **Error! Reference source not found.**, a risk assessment methods may be evaluated for the following purposes: (1) to establish its utility and efficacy for achieving its declared purpose; (2) to evaluate the method or theory supporting a risk assessment method; (3) to compare a risk assessment method with other methods in ability to achieve the same purpose; and (4) to identify weaknesses and ways for improvement of a risk assessment method.

The authors of risk assessment methods must be clear about which criterion they evaluate their method against. A “good” risk analysis method shall be (1) comprehensive, (2) adherent to evidence, (3) logically sound, (4) practical and politically acceptable, (5) open to evaluation, (6) based on explicit assumptions and premises, (7) compatible with the institutions, (8) conducive to learning, (9) attuned to risk communication, and (10) innovative **Error! Reference source not found.** Compliance with each of these ten criteria may be tested. A risk assessment method may also be evaluated regarding its fitness for purpose, ease to learn and use, the ability of the method to generate correct result, the effectiveness in achieving its goal, efficacy, ethicality, elegance and in terms of acceptance by practitioners [96, 95].

The Method Evaluation Model (MEM) **Error! Reference source not found.** is one of the possible frameworks to back up the evaluation of a risk assessment method. The MEM builds upon and adapts the Technology Acceptance Model (TAM) **Error! Reference source not found.** for the evaluation of system design methods and modelling languages. The TAM is a well accepted in the IS literature as a theoretical model for the evaluation of technology acceptance **Error! Reference source not found.** The MEM facilitates the empirical evaluation of the ease of use, usefulness and intention to use a method. Intention to use a method may serve as an indicator of whether the method might gain traction in industry.

A comparative evaluation of risk assessment methods for SCADA systems might demonstrate advantages and disadvantages of methods, and assist practitioners with the choice of the the suitable method. Over the last several years the MEM was actively used as a framework for the comparative evaluation of security and risk identification and analysis methods [98, 99, 101, 100].

6.5. *Supporting Risk Management Methods with Elaborate Tools*

The benefits of software tools supporting risk assessment and management activities are undisputed. Tools may facilitate data input for risk assessment in an intuitive user-friendly manner, automatically generate and analyse risk models, recommend security countermeasures or even trigger them as a response to undesired events.

The research on risk assessment in SCADA systems has not yet reached a level of

maturity where a software tool automating a method would be thoroughly elaborated and presented at length alongside the method. Software tools may ease the evaluation of methods by academics and industry experts. The feedback from testing may assist with the refinement of methods and tools in many aspects including unambiguous intuitive user interface, which is of no small importance in risk assessment tools. The evaluation of a method on real more complex cases and on a larger number of cases is less tedious when the risk assessment process is at least partially automated. Open access and open source risk assessment tools for SCADA systems could expedite the progress of the domain remarkably.

7. Conclusions

Over the years, we have seen a number of cyber attacks on CNI, ICS and SCADA systems (Section 2). The severity and consequences of attacks vary. Luckily, until now major disasters have mainly been averted. Unfortunately, without taking precautions we may not hope for this to happen in future as attackers get more sophisticated, experienced and malicious [93, Fig. 1].

It may seem that the probability of catastrophic cyber attacks on SCADA systems is relatively low (Section 1). This may lead to a false sense of security if we overlook two points.

First, considering the number of attacks, it is worth remembering that only a small number of security incidents is reported - *“Discussions with operators of traditional business crime reporting databases indicate that a typical incident database collects no better than one in ten of the actual events occurring”* **Error! Reference source not found..** Further, it is not possible to envision all possible attacks and the ways in which a SCADA system may fail. Resultantly, due to the inherent incompleteness of PRA methods, the actual value of the probability of cyber events occurrence is higher than estimated. For example, for incidents in power industry it was noted that *“While these may not be frequent in an absolute sense, there are good reasons to believe that they will be far more frequent than quantitative tools such as probabilistic risk assessments predict”* **Error! Reference source not found..** In line with the above, it is stated in **Error! Reference source not found.** that *“[c]omplex systems always retain the capacity to produce novel or surprising events.”*

Second, a potential loss from a cyber attack may be so severe that the risk, which is calculated as a product of the loss from the attack and the probability of the attack, is estimated as substantial even with a very low attack occurrence probability. Substantial risk calls for proportionate security investments.

The imperative importance of ensuring the cyber security of CNI and SCADA systems specifically is recognised in the UK. In September 2014, 2.5 million investment was made by the Engineering and Physical Sciences Research Council (EPSRC) and the UK’s National Cyber Security Programme into a new research project focusing on the cyber-security of the UK’s CNI. The project is supported by the Centre for the Protection of National Infrastructure (CPNI) and the Government Communications Headquarters (GCHQ). In April 2014, the Welsh Government and the EADS Foundation Wales invested in a new research project titled “SCADA Cyber Security Lifecycle”. The review paper at hand is one of the deliverables of this research project.

This paper contains a structured comprehensive overview of cyber security risk

assessment methods applied to SCADA systems. In this review, we followed a well-established literature search methodology and strived to made the literature review process transparent.

Overall, the contribution of this review paper is three-fold:

- A review of the state of art in risk assessment of SCADA systems,
- A new categorisation scheme for risk assessment methods, and
- An outline of the research challenges in the domain.

The review indicates that despite the fact that a large number of risk assessment methods for SCADA systems exists there is still room for further research and multiple improvements. Cyber security risk assessment methods for SCADA systems may be improved in terms of (1) addressing the context establishment stage of the risk management process, (2) overcoming attack- or failure orientation, (3) accounting for the human factor, (4) the capturing and formalisation of expert opinion, (5) the improvement of the reliability of probabilistic data; (6) evaluation and validation, and (7) tool support. We also see a need for a comprehensive method which would cover all sages of the risk management process and deal with all key risk management concepts consistently.

In the paper, we also outlined some approaches that might be taken to these challenges. The consistent addressing of the specified research challenges will enhance future research about cyber security risk assessment methods in the SCADA context. We invite well positioned researchers and practitioners to extend the list of the challenges, and to continue the discussion. Shared understanding of the challenges facing the domain will facilitate its rapid maturing.

Acknowledgements

This work is funded by the Airbus Group Endeavr Wales scheme under the SCADA Cyber Security Lifecycle (SCADA-CSL) programme.

References

- [1] NIST Special Publication 800-82 Guide to Industrial Control Systems (ICS) Security June 2011
- [2] V. Ijure, S. Laughter and R. Williams, "Security issues in SCADA networks," *Computers & Security*, vol. 25(7), 2006, pp. 498-506.
- [3] Cabinet Office. Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards. March 2010.
- [4] A. Daneels, W. Salter, CERN, Geneva, Switzerland, "What is SCADA?" International Conference on Accelerator and Large Experimental Physics Control Systems, Trieste, Italy, 1999.
- [5] E. Byres, M. Franz, and D. Miller, "The use of attack trees in assessing vulnerabilities in SCADA systems," In: *Proceedings of the International Infrastructure Survivability Workshop*, 2004.
- [6] H. Morgan, "Cyber Security Risk Management in the SCADA Critical Infrastructure Environment," *Engineering Management Journal*, vol. 25(2), 2013.
- [7] P. Ralston, J. Graham, J. Hieb, "Cyber security risk assessment for SCADA and DCS networks," *ISA transactions*, vol. 46(4), 2007, pp. 583-594.
- [8] S. Patel, R. Tantalean, P. Ralston and J. Graham, "Supervisory control and data acquisition remote terminal unit testbed," Intelligent Systems Research Laboratory technical report TR-ISRL-05-01, Department of Computer Engineering and Computer Science. Louisville, Kentucky: University of Louisville. 2005.

- [9] E. Luiijf, "Why are we so unconsciously insecure?" *International Journal of Critical Infrastructure Protection*, vol. 12, 2013; 6 (s 3-4), pp.179-181.
- [10] B. Miller and D. Rowe, "A survey SCADA of and critical infrastructure incidents," In Proceedings of the 1st Annual conference on Research in information technology. ACM, 2012.
- [11] J. Guan, J. Graham and J.Hieb, "A digraph model for risk identification and management in SCADA systems", Intelligence and Security Informatics (ISI), 2011 IEEE International Conference on, IEEE CP., 2011, pp. 150-155.
- [12] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, "SCADA security in the light of Cyber-Warfare," *Computers & Security*, vol. 31(4), 2012, pp. 418-436.
- [13] M. Cheminod, L. Durante, A. Valenzano, "Review of Security Issues in Industrial Networks," *IEEE Transactions on Industrial Informatics*, vol. 9(1), 2013, pp. 277-293.
- [14] R. Larkin, J. Lopez, J. Butts and M. Grimaila, "Evaluation of security solutions in the SCADA environment," *ACM SIGMIS Database*, vol 45(1), 2014, pp. 38-53.
- [15] H. Leith and J. Piper, "Identification and application of security measures for petrochemical industrial control systems," *Journal of Loss Prevention in the Process Industries*, vol. 26(6), 2013, pp. 982-993.
- [16] S. Park and K. Lee, "Advanced Approach to Information Security Management System Model for Industrial Control System," *The Scientific World Journal*, Hindawi Publishing Corporation, 2014.
- [17] G.N. Ericsson, "Information Security for Electric Power Utilities (EPU)-CIGR Developments on Frameworks, Risk Assessment, and Technology," *Power Delivery*, IEEE Transactions on, vol. 24(3), 2009, pp. 1174-1181.
- [18] M. McQueen, W. Boyer, M. Flynn, G. Beitel, "A quantitative cyber risk reduction estimation methodology for a Small SCADA control system," In Proceedings of the 39th annual hawaii international conference on system sciences, 2006.
- [19] S. Gold, "The SCADA challenge: securing critical infrastructure," *Network Security* 2009, vol. 8, 2009, pp. 18-20.
- [20] BS ISO/IEC 27005:2011-*Information technology. Security techniques. Information security risk management*.
- [21] BS ISO 31000:2009. *Risk management. Principles and guidelines*.
- [22] NIST. *Guide for Applying the Risk Management Framework to Federal Information Systems-A Security Life Cycle Approach*. NIST SP 800-37 rev. 1, 2010.
- [23] C. Chittester and Y. Y. Haimes, "Risks of terrorism to information technology and to critical interdependent infrastructures," *Journal of Homeland Security and Emergency Management*, vol. 1(4), 2004, article 402.
- [24] S. Kaplan and B. J. Garrick, "On the quantitative definition of risk," *Risk Analysis*, vol. 1(1), 1981, pp. 1137.
- [25] NISCC (CPNI). Firewall deployment for SCADA and process control networks good practice guide. 2005.
- [26] NERG. Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions. Available at <http://www.nerc.com/pa/stand/pages/project-2014-xx-critical-infrastructure-protection-version-5-revisions.aspx>.
- [27] K. Trivedi and R. Sahner, "SHARPE at the age of twenty two," *ACM SIGMETRICS Performance Evaluation Review*, vol. 36(4), 2009, pp. 52-57.

- [28] C. Alberts, A. Dorofee, J. Stevens and C. Woody, "Introduction to the OCTAVE Approach," Software Engineering Institute. August 2003.
- [29] NIST. Risk Management Guide for Information Technology Systems. Special Publication 800-30. July 2002.
- [30] B. Karabacak and I. Sogukpinar, "ISRAM: information security risk analysis method," *Computers & Security*, vol. 24(2), 2005, pp. 147-159.
- [31] S. Patel, J. Graham, P. Ralston, "Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements," *International Journal of Information Management*, vol.28(6), 2008, pp. 483-491.
- [32] P. Campbell, J. Stamp, "A classification scheme for risk assessment methods," Sandia National Laboratory, SAND2004-4233, 2004.
- [33] J. D. Markovic-Petrovic and M. D. Stojanovic, "An Improved Risk Assessment Method for SCADA Information Security," *Elektronika ir Elektrotechnika*, vol. 20(7), 2014, pp. 69-72.
- [34] V. Verendel, "Quantified security is a weak hypothesis: a critical survey of results and assumptions," In Proceedings of the 2009 workshop on New security paradigms workshop, ACM, 2009, pp. 37-50.
- [35] R. von Solms, "Can security baselines replace risk analysis?" Information Security in Research and Business. Springer US, 1997. pp. 91-98.
- [36] C. Taylor, A. Krings and J. Alves-Foss, "Risk analysis and probabilistic survivability assessment (RAPSA): An assessment approach for power substation hardening," In Proc. ACM Workshop on Scientific Aspects of Cyber Terrorism, (SACT), Washington DC, vol. 64. 2002.
- [37] G. Giannopoulos, R. Filippini and M. Schimmer, Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art. European Commission Joint Research Centre Institute for the Protection and Security of the Citizen Technical Notes. EUR 25286 EN-2012.
- [38] P. Kertzner, D. Bodeau, R. Nitschke, J. Watters, M. Young, M. Stoddard, "Process control system security technical risk assessment: Analysis of problem domain," I3P, Research report No.3, 2006.
- [39] B. Kitchenham and P. Brereton, "A systematic review of systematic review process research in software engineering," *Information and Software Technology*, 55(12), 2013, pp. 2049-2075.
- [40] T. Gopal, M. Subbaraju, R. Joshi and S. Dey, "MAR(S)2: Methodology to articulate the requirements for security In SCADA," Innovative Computing Technology (INTECH), 2014 Fourth International Conference on, 2014, pp. 103-108.
- [41] S. Jung, J. Song, S. Kim, "Design on SCADA Test-bed and Security Device," *International Journal of Multimedia and Ubiquitous Engineering*, vol. 3(4), October, 2008.
- [42] C. Ten, C. Liu and M. Govindarasu, "Cyber-vulnerability of power grid monitoring and control systems," In Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead, p. 43. ACM, 2008.
- [43] G. Hamoud, R. Chen and I. Bradley, "Risk Assessment of Power Systems SCADA," IEEE Power Engineering Society General Meeting, 13-17 July, vol. 2, 2003, pp. 758-764.

- [44] L. Briand, Khaled El Emam and F. Bomarius, "COBRA: a hybrid method for software cost estimation, benchmarking, and risk assessment," Proceedings of the 20th international conference on Software engineering. IEEE Computer Society, 1998.
- [45] Information Security Forum (ISF). Simplified practical risk analysis methodology (SPRINT) user guide, 1997, p. 43-57.
- [46] R. Coles and R. Moulton, "Operationalizing IT risk management," *Computers & Security*, vol. 22(6), 2003, pp. 487-493.
- [47] Z. Yazar, A Qualitative Risk Analysis and Management Tool - CRAMM. SANS Institute. 2002.
- [48] RiskWorld. <http://www.riskworld.net/>
- [49] J. Aagedal, D. Braber, T. Dimitrakos, B. Gran, D. Raptis and K. Stolen, "Model-based risk assessment to improve enterprise security," In Enterprise Distributed Object Computing Conference, 2002. EDOC'02. Proceedings. Sixth International, IEEE, pp. 51-62.
- [50] K. Stolen, Folker den Braber, T. Dimitrakos, R. Fredriksen, B. Gran, S. Houmb, M. Lund, Y. Stamatou and J. Aagedal, "Model-based risk assessment the CORAS approach," In 1st iTrust Workshop. 2002.
- [51] CPNI. Good Practice Guide Process Control and SCADA Security.
- [52] NIST. System Protection Profile-Industrial Control Systems. Version 1.0, October 29, 2004.
- [53] US Department of Energy, Infrastructure Security and Energy. 21 Steps to Improve Cyber Security of SCADA Networks - U.S. 2007.
- [54] ENISA. Window of exposure a real problem for SCADA systems? Recommendations for Europe on SCADA patching. December 2013.
- [55] N. Balasubramanian, C. Chang, and Y. Wang, "Petri-net models for risk analysis of hazardous liquid loading operations, *Industrial & Engineering Chemistry Research*, vol. 41(19), pp. 4823-4836, 2002.
- [56] Y. V. Haimes, "Hierarchical holographic modeling," *Systems, Man and Cybernetics*, IEEE Transactions on, vol. 11(9), 1981, pp. 606-617.
- [57] M. R. Permann and K. Rohde, "Cyber assessment methods for SCADA security," 15th Annual Joint ISA POWID/EPRI Controls and Instrumentation Conference, Nashville, TN, 2005.
- [58] M. McQueen, W. Boyer, M. Flynn, and G. Beitel, "Time-to-compromise model for cyber risk reduction estimation, in Proceedings of the 1st Quality of Protection Workshop at the University of Trento, Milan. Springer, 2005.
- [59] Y. Jiayi, M. Anjia and G. Zhizhong, "Vulnerability Assessment of Cyber Security in Power Industry," Power Systems Conference and Exposition (PSCE), IEEE, 2006, pp. 2200-2205.
- [60] D. Gertman, R. Folkers and J. Roberts, "Scenario-based approach to risk analysis in support of cyber security," In: Proceedings of the 5th International Topical Meeting on Nuclear Plant Instrumentation Controls, and Human Machine Interface Technology, 2006.
- [61] C. Beggs and M. Warren, "Safeguarding Australia from cyber-terrorism: a proposed cyber-terrorism SCADA risk framework for industry adoption" In Australian Information Warfare and Security Conference, December, 2009, p. 5.
- [62] M. H. Henry, R. M. Layer, K. Z. Snow and D.R. Zaret, "Evaluating the risk of

- cyber attacks on SCADA systems via Petri net analysis with application to hazardous liquid loading operations,” In: Technologies for Homeland Security, HST’09, IEEE Conference on, IEEE, 2009, pp. 607-614.
- [63] F. Baiardi, C. Telmon, and D. Sgandurra, “Hierarchical, model-based risk management of critical infrastructures, *Reliability Engineering & System Safety*, vol. 94(9), 2009, pp. 1403-1415.
- [64] M. Henry and Y. Haimès, “A comprehensive network security risk model for process control networks, *Risk Analysis*, vol. 29(2), 2009, pp. 223-248.
- [65] Y. Y. Haimès and B. M. Horowitz, “Adaptive two-player hierarchical holographic modeling game for counterterrorism intelligence analysis,” *Journal of Homeland Security and Emergency Management*, vol. 1(3), 2004, pp. 121.
- [66] M.H. Salinas, *Combining multiple perspectives in the specification of a security assessment methodology*. PhD. Thesis, University of Virginia, 2003.
- [67] A. Roy, D. S. Kim and K. S. Trivedi, “Cyber security analysis using attack countermeasure trees,” In: Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, ACM, 2010, p. 28.
- [68] E. LeMay, W. Unkenholz, D. Parks, C. Muehrcke, K. Keefe and W. H. Sanders, “Adversary-driven state-based system security evaluation,” In: Proceedings of the 6th International Workshop on Security Measurements and Metrics ACM, 2010, p.5.
- [69] E. LeMay, M. Ford, K. Keefe, W. Sanders and C. Muehrcke, “Model-based security metrics using adversary view security evaluation (advise),” In Quantitative Evaluation of Systems (QEST), 2011 Eighth International Conference on. IEEE. 2011, pp. 191-200.
- [70] D. Deavours, G. Clark, T. Courtney, D. Daly, S. Derisavi, J. M. Doyle, W. H. Sanders, and P. G. Webster, “The Möbius framework and its implementation, *IEEE Trans. on Software Engineering*, vol. 28 (10), 2002, pp. 956-969.
- [71] S. Patel and J. Zaveri, “A risk-assessment model for cyber attacks on information systems,” *Journal of Computers*, vol. 5(3), 2010, pp. 352-359.
- [72] C.-W. Ten, G. Manimaran, and C.-C. Liu, “Cybersecurity for critical infrastructures: Attack and defense modeling, *IEEE Trans. Syst., Man, Cybern.*, vol. 40(4), Apr. 2010, pp. 853-865.
- [73] A. Cardenas, A. Saurabh, Z. Lin, Y.n Huang, C. Huang and S. Sastry, “Attacks against process control systems: risk assessment, detection, and response,” In Proceedings of the 6th ACM symposium on information, computer and communications security, ACM, 2011, pp. 355-366.
- [74] L. Ricker, “Model predictive control of a continuous, nonlinear, two-phase reactor,” *Journal of Process Control*, vol. 3(2), 1993, pp. 109-123.
- [75] J. Song, J. Lee, C. Lee, K. Kwon, and D. Lee, “A cyber security risk assessment for the design of I&C Systems in nuclear power plants, *Nuclear Engineering and Technology*, vol. 44(8), 2012, pp. 919-928.
- [76] S. Kriaa, M. Bouissou, and L. Piètre-Cambacédés, “Modeling the Stuxnet attack with BDMP: Towards more formal risk assessments,” In Risk and Security of Internet and Systems (CRiSIS), 7th International Conference on, IEEE, 2012, pp. 1-8.
- [77] L. Piètre-Cambacédés, Y. Deflesselle and M. Bouissou, “Security modeling with BDMP: from theory to implementation,” In Network and Information Systems Security (SAR-SSI), 2011 Conference on, IEEE, 2011, pp. 1-8.

- [78] G. A. Francia III, D. Thornton and J. Dawson, "Security Best Practices and Risk Assessment of SCADA and Industrial Control Systems," In Proceedings of The 2012 World Congress in Computer Science, Computer Engineering, and Applied Computing, 2012.
- [79] J. Yan, M. Govindarasu, C.-C. Liu and U. Vaidya, "A PMU-based risk assessment framework for power control systems," Power and Energy Society General Meeting (PES), IEEE, 2013, pp. 1-5.
- [80] R. Hewett, S. Rudrapattana and P. Kijsanayothin, "Cyber-security analysis of smart grid SCADA systems with game models," In Proceedings of the 9th Annual Cyber and Information Security Research Conference, ACM, 2014, pp. 109-112.
- [81] P. S. Woo and B. H. Kim, "A Study on Quantitative Methodology to Assess Cyber Security Risk of SCADA Systems," In *Advanced Materials Research*, vol. 960, 2014, pp. 1602-1611.
- [82] D. J. Leversage and E. J. Byres, "Estimating a system's mean time-to-compromise," *Security & Privacy*, vol. 6(1), 2008, pp. 52-60.
- [83] G. Dondossola, F. Garrone, J. Szanto, "Supporting cyber risk assessment of Power Control Systems with experimental data," Power Systems Conference and Exposition, PSCE'09. IEEE/PES, 2009, pp. 1-3.
- [84] H. Lewis, R. Budnitz, W. Rowe, H. Kouts, F. Von Hippel, W. Loewenstein and F. Zachariasen, "Risk assessment review group report to the US Nuclear Regulatory Commission," Nuclear Science, IEEE Transactions on, 26(5), 1979, pp. 4686-4690.
- [85] E. Luijck, M. Ali and A. Zielstra, "Assessing and improving SCADA security in the dutch drinking water sector," In Critical Information Infrastructure Security, Springer Berlin Heidelberg, 2009, pp. 190-199.
- [86] G. Dondossola, F. Garrone, J. Szanto, "Cyber risk assessment of power control systems-A metrics weighed by attack experiments," Power and Energy Society General Meeting, IEEE, 2011, pp. 1-9.
- [87] T. Morris, R. Vaughn and Y. Dandass, "A testbed for scada control system cybersecurity research and pedagogy," In Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research, ACM, 2011, p. 27.
- [88] Z. Tudor and M. Fabro, "What Went Wrong? A Study of Actual Industrial Cyber Security Incidents," Industrial Control Systems Joint Working Group (ICSJWG) Spring Conference. 2010.
- [89] M. V. Ramana, "Beyond our imagination: Fukushima and the problem of assessing risk," *Bulletin of the Atomic Scientists*, 2011.
- [90] RISI, "Industry Attacks Growing," October 14, 2013. Available: <http://www.isssource.com/risi-industry-attacks-growing>. Accessed: 23/01/2015.
- [91] E. Byres, D. Leversage and N. Kube, "Security incidents and trends in SCADA and process industries," The Industrial Ethernet Book, vol. 39(2), 2007, pp. 12-20.
- [92] CPNI. Information exchanges. Available: <http://www.cpni.gov.uk/about/who-we-work-with/information-exchanges>.
- [93] Y. Y. Haimes and C. G. Chittester, "A roadmap for quantifying the efficacy of risk management of information security and interdependent SCADA systems," *Journal of Homeland Security and Emergency Management*, vol. 2(2), 2005, pp. 121.
- [94] The Open Group. Dependency Modeling (O-DM). Constructing a Data Model to Manage Risk and Build Trust between Inter-Dependent Enterprises. Open Group

Standard. 2012.

[95] Moody, D. L. (2003, June). The method evaluation model: a theoretical model for validating information systems design methods. In 11th European Conference on Information Systems, ECIS.

[96] J. Venable, J. Pries-Heje and R. Baskerville, A Comprehensive Framework for Evaluation in Design Science Research. Design Science Research in Information Systems. Advances in Theory and Practice Lecture Notes in Computer Science. (eds K. Peffers, M. Rothenberger and B. Kuechler), Springer Berlin / Heidelberg. 2012, pp. 423-438.

[97] Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology Author(s): Fred D. Davis Reviewed work(s): Source: MIS Quarterly, Vol. 13, No. 3 (Sep., 1989), pp. 319-340.

[98] K. Labunets, F. Massacci, F. Paci, L. Tran, "An experimental comparison of two risk-based security methods," Empirical Software Engineering and Measurement, 2013 ACM/IEEE International Symposium on. IEEE, 2013, pp. pp. 163-172.

[99] K. Labunets, F. Paci, F. Massacci, R. Ruprai, "An experiment on comparing textual vs. visual industrial methods for security risk assessment. Empirical Requirements Engineering (EmpiRE), 2014 IEEE Fourth International Workshop on. IEEE, 2014, pp. 28-35.

[100] S. Espaná, N. Condori-Fernandez, A. González, Ó. Pastor, "An empirical comparative evaluation of requirements engineering methods," *Journal of the Brazilian Computer Society*, 16(1), 2010, pp. 3-19.

[101] B. Fabian, S. Grses, M. Heisel, T. Santen, H. Schmidt, "A comparison of security requirements engineering methods," *Requirements engineering*, 15(1), 2010, pp. 7-40.

Figure 1: Generic SCADA hardware architecture. NIST SP 800-82 [1, p.2-7]

Figure 2: Attack tree for a MODBUS-based SCADA system

(excerpt) **Error! Reference source not found.**

Figure 3: An attack step [68, 69]

Figure 4: The number of papers per year

Figure 5: Risk management process **Error! Reference source not found.**

Table 1: List of the Risk Assessment Methods for SCADA Systems (ordered by the number of citations)

No.	Ref.	Year	Method Title	Country	Citations
1	Error! Reference source not found	2011	Risk Assessment, Detection, and Response	USA	104
2	Error! Reference source not found	2010	Cybersecurity for Critical Infrastructures: Attack and Defense Modeling	Ireland	87
3	Error! Reference source not found	2004	Attack Trees for Assessing Vulnerabilities	Canada	85

			in SCADA		
4	Error! Reference source not found	2006	Quantitative Cyber Risk Reduction Estimation Methodology	USA	44
5	Error! Reference source not found	2008	Two Indices Method for Quantitative Assessment of the Vulnerability of Critical Information Systems	USA	31
6	Error! Reference source not found	2004	Risk Assessment in GPS-based SCADA for Railways	USA	26
7	Error! Reference source not found	2009	Hierarchical, Model-Based Risk Management of Critical Infrastructures	Italy	26
8	Error! Reference source not found	2010	Adversary-Driven State-Based System Security Evaluation	USA	21
9	Error! Reference source not found	2010	Attack Countermeasure Tree	USA	19
10	Error! Reference source not found	2006	Vulnerability Assessment of Cyber Security in Power Industry	China	12
11	Error! Reference source not found	2012	Boolean logic Driven Markov Processes (BDMP)	France	10
12	Error! Reference source not found	2005	Vulnerability Assessment Methodology for SCADA Security	USA	9
13	Error! Reference source not found	2009	Network Security Risk	USA	8

			Model (NSRM)		
14	Error! Reference source not found	2009	Evaluating the Risk of Cyber Attacks on SCADA Systems via Petri Net Analysis	USA	7
15	Error! Reference source not found	2010	Risk-Assessment Model for Cyber Attacks	USA	7
16	Error! Reference source not found	2012	Cyber Security Risk Assessment in Nuclear Power Plants	Korea	6
17	Error! Reference source not found	2009	Cyber-Terrorism SCADA Risk Framework	Australia	2
18	Error! Reference source not found	2012	CORAS-based Risk Assessment for SCADA	USA	2
19	Error! Reference source not found	2011	Digraph Model for Risk Identification and Management in SCADA Systems	USA	1
20	Error! Reference source not found	2013	PMU-based Risk Assessment Framework for Power Control Systems	USA	1
21	Error! Reference source not found	2006	Scenario-based Approach to Risk Analysis in Support of Cyber Security	USA	0
22	Error! Reference source not found	2014	Improved Risk Assessment Method for SCADA Information Security	Serbia	0
23	Error! Reference source not found	2014	Cyber-Security Analysis of Smart Grid SCADA	USA	0

			Systems with Game Models		
24	Error! Reference source not found	2014	Quantitative Methodology to Assess Cyber Security Risk of SCADA Systems	Korea	0

Table 2: Categorisation of the Methods by the Level of Detail and Coverage

Level of detail Coverage	High	Low
Broad	Elaborated guidelines [18, 60, 63, 64, 72, 79]	Guidelines [57, 61, 75]
Narrow	Activity-specific methods [5, 11, 23, 33, 59, 31, 62, 67] [68, 71, 73, 76, 78, 80, 81]	

Table 3: Categorisation of the methods into qualitative and quantitative

Category		References
Qualitative		[23, 5, 61, 75, 78]
Quantitative	Probabilistic	[18, 33, 59, 60, 31, 63, 64, 67, 68, 71, 72, 76, 79, 80]
	Non-Probabilistic	[62, 11, 81]
	Not specified	[57]

Table 4: Categorisation of the methods into formula-based and model-based

Category	References
Formula-based	[59, 60, 71, 73, 33, 81]
Model-based	Error! Reference source not found. - attack tree with characteristics of attack goals/nodes (A) Error! Reference source not found. - directed graph of a system (G) Error! Reference source not found. - compromise graph (A) Error! Reference source not found. - HHM (G) Error! Reference source not found. - vulnerability tree with threat-impact and cyber-vulnerability indices (A) Error! Reference source not found. - Petri Net (A) Error! Reference source not found. - hypergraph and evolution graph (D) Error! Reference source not found. - directed attack graph (A) Error! Reference source not found. - attack tree with adversary profile (A) Error! Reference source not found. - attack tree with countermeasures (A) Error! Reference source not found. - attack graph with system-, scenario-, and leaf-level vulnerability indices (A) Error! Reference source not found. - attack graph with probabilities of events (A) Error! Reference source not found. - game tree (game theory) (A) Error! Reference source not found. - fault tree with Markov processes with probabilities and success rates (A)

	Error! Reference source not found. - CORAS modelling language (A)
--	--

(A) - attack- or failure-oriented approach

(G) - goal-oriented approach

(D) - dual approach

Table 5: Categorisation of the Methods by the Source of Probabilistic Data

Source	References
None or not applicable	[23, 57, 61, 62, 11, 75, 78]
Applicable, but not specified	[59, 67, 73, 73, 79]
Historical data	[63, 72, 33]
Experts opinion	[5, 18, 68, 71, 76]
Experts opinion & historical data	[60, 31, 64, 80, 81]

Table 6: The overview of the Risk Assessment Methods

Ref.	Domain	Aim	Evaluation
DisplayText cannot span m	Rail road sector	Identify sources of risk	NO
DisplayText cannot span m	Energy sector	Calculate the characteristics of the topmost attack event	Initial settings are validated by energy sector operators; the feasibility of attacks is tested in a laboratory setting
DisplayText cannot span m	Energy sector	Identifying vulnerabilities and assessing security of SCADA systems	NO
DisplayText cannot span m	Small SCADA	Calculate risk reduction in a security enhanced SCADA system	Real life case study
DisplayText cannot span m	Energy sector	Calculate cyber vulnerability index	NO
DisplayText cannot span m	Nuclear plant	Help decision makers with the allocation of financial and personnel resources to more critical attacks	Generic case study
DisplayText cannot span m	Tank and pump	Help system managers to	Case study on a test SCADA system

	system	make informed decisions about security countermeasures	
DisplayText cannot span more than one line	Generic SCADA	Measure and protect SCADA systems from the threat of cyber-terrorism within Australia	Focus group of five SCADA engineering consultants
DisplayText cannot span more than one line	Hazardous liquid loading process	Measure operational risk using non-probability-based metrics	Case study based on the system described in DisplayText cannot span more than one line
DisplayText cannot span more than one line	Generic SCADA	Automate definition of risk mitigation plan	Generic example
DisplayText cannot span more than one line	Crude oil pipeline pump station	Assist with the selection of risk management controls	Illustrative example on a simplified version of the system
DisplayText cannot span more than one line	Generic SCADA	Generation of attack scenarios and selection of the optimal set of countermeasures	Generic example of a SCADA attack analysed using SHARPE and MATLAB
[68, 69]	Electric power sector	Simulate an attack on a system and calculate the probability of the success of the attack	Examples from a generic electric power SCADA system, generic example from DisplayText cannot span more than one line
DisplayText cannot span more than one line	Chemical plant	Calculate a total estimated revenue loss from all cyber attacks	Real- world case study of a chemical engineering plant
DisplayText cannot span more than one line	Energy sector	Hypothetically evaluate the	Application on a test subnet of electric power control

		system vulnerability level in a simplified way	network
DisplayText cannot span multiple lines	Chemical distillation column	Assess risk impact, diagnose faults and identify vulnerabilities	Case study on a laboratory scale distillation column
DisplayText cannot span multiple lines	Chemical reactor system	Identify high priority sensors for prioritising security budget	Laboratory experiments
DisplayText cannot span multiple lines	Nuclear power plant	Outline the risk assessment activities at the system design stage	Example of a digital reactor protection system
DisplayText cannot span multiple lines	Stuxnet attack	Attack modelling, and enumeration and quantification of the possible sequences of attack steps	Model of the Stuxnet attack
DisplayText cannot span multiple lines	Generic SCADA	Risk modelling of a prototypical ICS using CORAS	Case study
DisplayText cannot span multiple lines	Power grids	Monitor the impact of cyber intrusions on power system dynamics in real time	Simulation
DisplayText cannot span multiple lines	Hydro-power plant	Calculating how effective intrusion, detection and prevention systems are for preventing attacks	Case study
DisplayText cannot span multiple lines	Smart	Calculate	Case study of a sensor

	grid	payoffs and find best action strategy for attacker and defender	network SCADA
DisplayText cannot span n	Smart grid	Calculate expected damage from a cyber threat	Case study

Table 7: Stages of the Risk Management Process Addressed by the Methods

Ref.	Context Establishment	Risk Identification	Risk Analysis	Risk Evaluation	Risk Treatment	Metrics analysed/measured
Display	●				●	SCADA system submodels, element and subtopics, control objectives
Display		●	●			Attacker goals, resources required for an attack, severity of impact and detection probability
Display		●				Hardware, software and network vulnerabilities
Display		●	●	●		Attack scenarios, vulnerabilities and time-to-compromise
Display			●			Vulnerability index
Display		●	●			Attack variations, attacker skills, impact
Display		●	●	●		Vulnerability, threat-impact index and cyber-vulnerability index
Display		●			●	Terrorist cyber-capability level, terrorist motivation
Display		●	●			Process failure modes, failure consequences, attacker resources,
Display	●	●	●		●	Security dependency among the components of a system, attack strategies, the optimal set of countermeasures
Display	●	●	●	●	●	Infrastructure, failure modes and effects, processes, attack scenarios, network structure and access requirements
Display		●	●		●	Attack scenarios, cost and impact of an attack, optimal countermeasure set
Display		●	●	●		Attack graph, characteristics of adversary

Displa		●	●			Attack type, revenue loss
Displa	●	●	●		●	Cybersecurity conditions, intrusion scenario,s vulnerability indices, port risk factor, password strength, security improvements
Displa	●	●				Structure and behaviour of a system, fault propagation paths
Displa		●	●		●	Attack model, linear model of the behaviour of a system, anomaly detection algorithm
Displa	●	●	●		●	Security modelling, asset, impact, threat, vulnerability, security control design and penetration test
Displa		●	●			Attack steps sequences
Displa	●	●				Asset, vulnerability, and human and non-human threat modelling
Displa	●	●	●	●	●	Attack graph
Displa			●	●		Loss expectancy and return on investment
Displa		●	●		●	Payoff, impact
Displa	●	●	●			Asset value, threat, vulnerability, impact

Table 8: Key Risk Management Concepts Addressed by the Methods

Ref.	System/ Asset	Vuln erabi lity	Threat/ Attack	Countermea sure	Impact	Impact Measurement
Displa	●			●		N/A
Displa		●	●		●	Level of severity on a relative scale
Displa		●				N/A
Displa		●	●	●		N/A
Displa					●	Monetary
Displa		●	●		●	Monetary and human lives
Displa		●	●	●	●	Monetary
Displa			●	●		N/A
Displa		●	●		●	Number of injures
Displa	●	●	●	●	●	Not specified
Displa	●	●	●	●	●	Gallons of crude oil lost flow per day
Displa			●	●	●	Monetary
Displa			●			N/A
Displa			●		●	Monetary
Displa	●	●	●	●	●	Numeric index

Displa	●					N/A
Displa		●	●	●		N/A
Displa	●	●	●	●	●	List of system components affected
Displa			●			N/A
Displa	●	●	●			N/A
Displa	●	●	●	●	●	Voltage instability
Displa					●	Monetary
Displa			●	●	●	Numeric index
Displa	●	●	●		●	Monetary